Communications & Operations Management Policy

PART ONE: PURPOSE & SCOPE, RESPONSIBILITIES

1 Policy Statement
The Council and Trusts will protect IT and Communications services and systems (ICT) from malicious attack.

Only authorised changes will be made to ICT

Information leakage will be prevented by secure controls.

2 Purpose
This policy specifies the Council and Trust’s mandatory minimum security standards for the management of:
- ICT operations
- Systems development
- Change
- Day to day operations
- Operational procedures.

This policy should be applied whenever users access Council or Trust IT facilities and equipment, and especially when managing, developing, configuring or maintaining these facilities and equipment.

3 Scope
This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, Employees of local Trusts providing services on behalf of LBC, contractual third parties and agents of the Council and Trusts who use Luton Borough Council provided IT facilities and equipment, or have access to, or custody of, Council or Trust customer information.

All users must understand and adopt this policy and are responsible for ensuring the safety and security of the Council’s systems and the information that they use or manipulate.

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.
PART TWO: POLICY

3.1 Operational Procedures and Responsibilities

3.1.1 Documented Operating Procedures

Operating procedures are used in all day to day maintenance of Council and Trust ICT in order to optimise service delivery from these assets. These operating procedures must be documented to an appropriate level of detail for the departmental team that will be using them.

3.1.2 Change Management

All Changes to Council and Trust operational systems must be controlled with formally documented change control processes. These processes will reference and where necessary comply with:

- Government Connect Code of Connection (Co-Co)
- IT Infrastructure Library (ITIL) Change Management practices
- Local Government Data Handling guidelines
- ISO27001:2005 Information security management standard

Change control requirements are defined within the separate Information Management Change Control Policy.

Key components of this policy are

- A description of the planned 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.

It is the responsibility of the Asset Owner to ensure that when changes are undertaken by a third party on behalf of the Council or Trust, equivalent change control processes will be agreed and applied.

3.1.3 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, but not limited to, the following:

- Test and operational hosted in separate environments such as separate computers (virtual or physical), domains or networks.
- Separate usernames and passwords will be used for these separate environments.
- Separation of duties will exist to limit access between test and operational systems.

It is the responsibility of the Asset Owner to ensure that when development and testing is undertaken by a third party on behalf of the Council or Trust, equivalent change control processes will be agreed and applied.

3.2 System Planning and Acceptance
3.2.1 Capacity Planning

A capacity planning strategy including the capture of changes in demand and regular reporting of key trends will exist in relation to:

- Power requirements
- Processing requirements
- Storage requirements

The strategy will monitor growth on ICT components such as:

- File servers
- Storage Area Networks (SANs)
- Domain Controllers
- E-mail servers
- Web servers
- Printers
- Network traffic
- Environmental controls including air conditioning

This list is not exhaustive

3.2.2 System Acceptance

All departments must inform Information Management (IM) 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 IM Acquisitions as defined in the ‘Software Policy.

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.

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

It is the responsibility of the Asset Owner to ensure that when System, delivery is undertaken by a third party on behalf of the Council or Trust, equivalent Systems acceptance processes will be agreed and applied

3.2.3 Public facing systems

Where any Council or Trust application is to be presented to the internet, to a public subscriber network or to another network not controlled by the Council, then it is deemed a ‘public facing system’ and must be security tested prior to going live

Where such applications are upgraded they must again be hardened, patched and security tested.

Hardening is a process whereby unnecessary features and services are removed from the application and the infrastructure hosting the application thus minimizing the number of features an attacker could exploit.

Patching is a process where by known weaknesses within the application are fixed.
Processes for Hardening and patching of ICT assets including public facing applications is defined within the Information management ‘Hardening and patching policy’

Security testing will take the form of an ‘application vulnerability assessment’ to determine whether the application contains any weakness that might either, grant someone the opportunity to access or damage systems of information on the Council’s private network or to access or damage the public facing application itself or the infrastructure that supports it.

Where a public facing application receives a minor upgrade or patch only, the security test need not occur prior to the application going live, however security testing must occur be undertaken during the next scheduled corporate penetration test (a wide-scale test of Council and Trust information security undertaken by a trusted 3rd party at least annually).

A record of all patches and upgrades to public facing systems hosted via the Council’s private network will be held by Information Management

Where a weakness in any public facing is found this will addressed as described in the Information Management ‘hardening and Patching policy’.

Where a weakness is found, an application may not be permitted to go live, may be removed from service or may be given a time limit for the issue to be resolved after which it will be removed from service. Guidance on the decision making process behind this is contained within the Information Management ‘Hardening and Patching policy’.

All security tests (application vulnerability assessments and penetration tests) will be arranged through Information Management

It is the responsibility of the Asset (public facing application) Owner to ensure that when System, delivery is undertaken by a third party on behalf of the Council or Trust, equivalent Security testing processes are agreed and applied

3.3 Protection against Malicious and Mobile Code

Appropriate steps are taken to protect all Council and Trust ICT from malicious code (viruses, malware or programmes designed to compromise security in some shape or form).

Effective and up-to-date anti-virus software will be run on all servers and PCs. Any exceptions to this will require a business case to be documented, approved by the Head of Information management and logged for future reference

Council and Trust users are responsible for ensuring that they do not introduce malicious code into IT systems. Users must therefore check regularly to ensure that Anti-virus software on their computer(s) is current and fully functional. Users must scan all removable media for viruses as described in the ‘removable media policy.

Where a virus or malware is detected the event will be reported to the IM service desk ‘6666’ at the earliest practical opportunity as described in the ‘Information Security Incident management Policy.’
Users must not attempt to change or remove anti-virus software as described the ‘Software Policy’

3.3.1 Threats posed by malicious Mobile Code

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

- ActiveX.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.

These technologies can be exploited to facilitate various threats to the Council’s private network and the information and systems within it, consequently these technologies are limited, with their use prohibited, mitigated by virtue of other controls or permitted only where there is a business case.

3.3.2 Controls against malicious Mobile Code

Controls will exist to prevent the infection or propagation of malicious and mobile code, appropriate access controls. These controls will include:

- Limitation of user access rights as described in the ‘Access Control Policy’
- Limitations on use of the following technologies except where permitted by a business case approved by the Senior Information Risk Officer (SIRO):
  - ActiveX
  - Active content e.g. JavaScript and VB script
  - HTTPS
  - Java Virtual machine (JVM)
- At least 2 separate Anti virus software products will exist on the Council's private network, e.g. product A will scan traffic emanating from the Internet or other untrusted networks, while product B will scan files on desktop computers, laptops and removable media.
- Software may only be purchased and installed in compliance with the ‘Software Policy’

3.3.3 Patching

Patching processes and standards for all Council and Trust ICT infrastructure and applications are defined within the Information Management Patching policy

3.4 Backups

3.4.1 Information backup, transportation, storage, recovery and disposal

Back-up
Regular backups of essential business information must be taken

An appropriate backup cycle must be used and fully documented
Full backup documentation, including a complete record of what has been backed up along with copies of back-up media such as back-up tapes or cartridges must be stored and readily accessible

Local service continuity plans will be maintained and tested by individual Council and Trust Departments and Services as detailed in the ‘Business Continuity Policy’

Storage of backup media and documentation
Backup documentation, backup media and restore/recovery documentation must be held securely in at least 2 locations as follows:

- Council or Trust premises; this must be an enhanced secure location as described in the ICT Infrastructure Security policy (typically an Information Management Data centre).
- A secure off site location that is sufficiently remote to avoid being affected by any disaster that takes place at the main site.

Minimum standards for secure storage of back up media on and off site are as follows:
- Access to the media will be restricted to designated Council or Trust personnel
- Back-up media and documentation will be stored in an ‘enhanced secure area’ as described within the ICT Infrastructure Security Policy.

Transportation of backup media and documentation
Backup media must be protected from unauthorised access, misuse or corruption during transportation.

Physical controls such as encryption or special locked containers should be used

Backup media may only be transported:

- Securely, in person by designated Council or Trust personnel
- Securely, in person by authorised employees of a secure off site storage provider
- Via a 3rd party courier service, where the company is known and trusted by the Council or Trust and where the media will not leave the original delivery vehicle until signed for at the point of destination
- On completion of transit backup media will be stored securely

Backup media may not be transported by any methods other than described above

3.4.2 Disposal of Storage Media

Storage media that is obsolete or no longer required must be destroyed in a secure and environmentally friendly manner. This must include thorough removal of all data from the storage media to avoid the potential of data leakage.

Council and Trust Information held by a third party

It is the responsibility of the Asset Owner to ensure that where information is stored by a third party on behalf of the Council or Trust, equivalent back-up, storage transit, recovery and disposal regimes are agreed and applied.

3.5 Monitoring

3.5.1 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. 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.

3.5.2 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.

3.5.3 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.

3.6 Network Management

3.6.1 Network Controls

Connections to the Council’s private 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 (see remote and mobile working policy, removable media policy, and Information Management procedure manual for Networking & Communications).
• 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.
3.6.2 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. Co-Co minimum mandatory requirements will be adhered to in configuration of any wireless network functionality.

3.7 Systems Development and Maintenance

3.7.1 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 (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.

3.8 Annual Health Check

An annual health check of all Council IT infrastructure systems and facilities must be undertaken by Information Management 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.
Policy enforcement
The interpretation and application of this policy in relation to any alleged non-compliance will be undertaken as follows:

<table>
<thead>
<tr>
<th>Alleged non-compliance by:</th>
<th>Interpretation and enforcement by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council employees</td>
<td>Council HR and Head of Service</td>
</tr>
<tr>
<td>Trust employees</td>
<td>Council/Trust HR and Trust Chief Executive</td>
</tr>
<tr>
<td>Council members</td>
<td>Council’s Monitoring Officer and Head of Local Democracy</td>
</tr>
<tr>
<td>Contractors or partner organisations</td>
<td>Contract/relationship manager and contracting organisation/partner</td>
</tr>
<tr>
<td>Staff Agencies</td>
<td>Contract/relationship manager and Council/Trust HR</td>
</tr>
<tr>
<td>Visitors or guests</td>
<td>Relevant Department HR</td>
</tr>
</tbody>
</table>

Breaches of this policy will be subject to Council or Trust disciplinary policy and procedures, contractual terms and conditions and civil and criminal law as appropriate.

If you do not understand the implications of this policy or how it may apply to you, please seek advice by submitting an e-mail enquiry to the IM service desk ‘6666’ in the first instance.

4 Policy Governance
The following table identifies who within Luton 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.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Head of Information Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Council’s Senior Information Risk Officer (SIRO)</td>
</tr>
<tr>
<td>Consulted</td>
<td>Information Steering group (ISG), Human Resources, legal services, Communications, Departmental representatives, Trust representatives, Employee Relations forum, Corporate Leadership Management team (CLMT), Unions, employee representatives, Representatives of Council members and</td>
</tr>
</tbody>
</table>
**APPENDIX 8**

**Communications and Operation Management Policy**

<table>
<thead>
<tr>
<th>special interest groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Informed</strong></td>
</tr>
<tr>
<td>All Council employees, Trust employees, Council members, temporary staff and contractors, suppliers and partner organisations.</td>
</tr>
</tbody>
</table>

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

Policy review will be undertaken by the Head of Information Management or their delegate.

**5 Definitions**

The Council - Luton Borough Council

The Trust - Active Luton, Luton Cultural Services Trust

ICT - Information and Communications technologies

Asset Owner - All Information and Systems will be assigned an Owner (see Information Classification and handling policy) who will be responsible for the security of that particular Information asset

Council’s Private Network – ICT network or network components that are reserved for use of Council and Trust users and not available to the general public

**6 References**

Legal and statute and mandatory requirements
- Data Protection Act 1998
- Government Connect Code of Connection (Co-Co)

Other guidelines and documents referenced by this policy
- Local Government Data Handling Guidelines
- ISO27001:2005 Security standard
- Central Government criteria for protective marking
- Software Policy
- Information Management Change Control Policy
- Information Management Hardening and Patching policy
- Removable media policy
- IT Infrastructure security policy