Loughborough University

Information Security

IT Operations Management Policy

Version 1.1:
Approved January 2022
Review May 2025

IT Operations Management Policy

1. Policy Overview

The University makes extensive use of computer and information systems for handling and processing information to support its business functions. It is the policy of the University that the systems it uses, and the information it manages, shall be appropriately secured.

This document contains the following policies to ensure that the underlying network and information systems, which use this network, are secure:

- Operations Management;
- Network Management;
- Systems Management;
- Vulnerability Management;
- Software Management;
- Encryption (Cryptography).

2. Policy Audience

This policy document contains technical details on how to manage a secure IT environment and is primarily aimed at IT Service and Park IT professionals across the University.

3. Operations Management

Purpose

This section outlines the requirements for the implementation and maintenance of a secure and resilient operational environment.

This sub policy applies to all computers, mobiles, tablets, and communications devices owned or operated by the University and any computer, mobiles, tablets, or communications devices that are present on the campus network.

Policy

Physical threats to security include:

- Environmental threats – temperature, humidity, fires, floods, storms;
- System threats – disruption to energy supply, communications;
- Human threats – unauthorised access, tampering, theft, wilful damage, accidents.

If buildings are being modified or essential maintenance work is being undertaken, the risks that construction work may present to information systems they house must be addressed and managed in collaboration with Facilities Management.

Data centre areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff which are authorised to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

The procedures for the operation and administration of all systems and activities forming part of or related to the University's information systems must be documented by those responsible for them, these procedures and documents shall be reviewed at appropriate intervals.

Changes to operational procedures must be controlled to ensure on going compliance with the requirements of information security and must have management approval.

Duties and areas of responsibility shall be appropriately segregated to reduce the risk and consequential impact of information security incidents that might results in financial or other material damage to the University.

Development and testing facilities for business-critical systems shall be logically separate from operational facilities and the migration of change from development to operational status shall be subject to IT Services change management process.

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the systems carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of data are in place.

Procedures shall be established to control the development and deployment of all operational systems.

Reporting of IT security incidents and suspected weaknesses in the University's business systems, should be reported to IT Service helpdesk either via email it.services@lboro.ac.uk or by calling 01509 222 333.

High Value Security Risk Areas

Where a room contains core-networking equipment, such as core routers (not regular communication locations which only contain edge switching), only authorised Pstaff should have access.

Rooms which hold high value and sensitive communications equipment (network core devices and where data is at rest) should meet the following specification:

- Masonry walls or studding reinforced with steel mesh;
- Metal door and frame to insurance LPS-1175 standard:
  - If internal door with an alarm on level 1;
  - f external door with no alarm on level 2;
  - If external door with no alarm on level 3;
- High security lock cylinder;
- Metal security bars to any windows;

- Cooling to match communications equipment load;
- Proximity card access with PIN keypad;
- Sounder if door is left open;

- Electronic door lock with record of visitor via electronic key safe;
- Security alarm panel;
- Intruder PIR movement detectors;
- Trembler alarms on walls;
- Remote alarm interface unit (or equivalent);
- CCTV covering external view of the door;
- CCTV covering internal view of the door;
- PIR control of lighting;
- IT cabinets with lockable doors (where possible);

4. Network Management

Purpose

The University network is a fundamental service that provides interconnects between all of the University's computing resources. It is vital that such a resource is properly controlled, maintained and managed. The purpose of this section covers the management, operation and use of the University data network.

This sub policy refers to the University network managed by IT Services, including the wireless network. The University network covers all building on the campus including student halls of residence (Hallnet) and remote locations such as Loughborough University London. Also covered is the protection of networked services to ensure that users who access the network and networked services do not compromise the security of these services.

Management

The Network and Communications team within IT Services is responsible for the University's campus network.

The University network shall be managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security, (confidentiality, integrity, availability). All network management staff shall be given relevant training in information security.

Other IT Specialists may undertake network moves if the Networks and Communication team has provided relevant training and an agreement is in place.

Switch based reconfigurations of a users' network will only be carried out by staff from the Networks and Communications Team within IT Services.

The implementation of new equipment or upgrades to network software or firmware must be carefully planned tested and managed. The Change Advisory Board must approve any changes.

Administrator passwords for all network devices must be set (or changed if a default one is present) to a complex password or passphrase which comprises of greater than 24 character and tested to confirm it has been applied.

AAA (triple A) (authentication, authorisation, and accounting) methodology must be implemented on network devices wherever possible using technologies such as RADIUS and TACAS+.

Where there is a risk to network security, quality of service for network users, or in order to enforce University policy, IT Services is authorised to:

- Impose restrictions on network traffic or use of network applications;
- Refuse connection of devices to the network;
- Remove networked devices or sub-sections of the network from service;
- Manage network resource allocation (e.g. bandwidth).

Monitoring

Network appliances or devices, which are critical to providing networking services to end-users must be monitored to ensure they are performing as expected.

Servers managed by the Networks and Communications Team, which provide network related services must be monitored to ensure the services are performing as expected.

Where the status of a monitored appliance, device, server or service changes to be critical an automated email alert must be sent to the Networks and Communications Team.

For the purpose of monitoring bandwidth across the campus network, links to and from all routers will be monitored, graphed and reviewed on a regular basis.

All servers centrally managed by IT Services providing services must be backed up using the backup solution provided by IT Services.

Where other IT Specialists manage servers, it is the responsibility of the service manager to ensure appropriate backups are taken at regular intervals.

All network appliances and devices must be able to back up their configuration to a central location, which must be maintained for a minimum of seven days.

Logging from network appliances and devices must be forwarded to a central location and stored for a minimum of thirty days.

Network design and configuration

The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University's business needs, whilst providing a high degree of control over access.

The network should be segregated where appropriate into separate logical sub-networks taking into account security requirements, with routing and access control lists operating between the sub-networks. Appropriately configured firewalls and other security mechanisms where appropriate shall be used to protect the sub-networks supporting the University's business critical systems.

Local area networks (LANs) in individual buildings, or extensions to them should only be designed and installed by IT Services.

IT Services is responsible for providing the enterprise wireless network service. Schools or Professional Services are prohibited from establishing their own wireless network and adding wireless access points unless authorised to do so by the Networks and Communication Team. This is to ensure the security, integrity and resilience of the wireless service is maintained.

IT Services reserve the right to make changes to network security as and when necessary. This may be in relation to a security threat or to improve existing arrangements.

Formal change control procedures, with a full audit trail, shall be used for all changes made to the University network infrastructure. All such changes must be risk assessed and authorised by the relevant manager before being making configuration changes.

Security and resilience

Reasonable measures based on a risk assessment, such as fire and water protection, locked dedicated space, secure cabinets etc, must be taken to protect networks and communication equipment against accidental damage, security breaches, theft or malicious intent.

The network should where possible incorporate logical and physical resilience features to help mitigate against the impact of failure or physical damage to cabling and other network equipment.

Firmware updates/patches for networking devices which address critical and/or high vulnerabilities must be installed within 14 days of release.

Network services and protocols

Only IT Services will manage the IP address space (IPv4 and IPv6), which has been allocated to the University and operate Dynamic Host Configuration Protocol (DHCP) service to issue IP addresses.

IP address blocks allocated to schools will be managed by Part IT staff using the “Hostbuilder” tool provided by the Networks and Communications Team.

The Networks and Communications Team within IT Services manages IP routing protocols running on the University’s core routers. Routing protocols such as EIGRP, OSPF, ISIS should be disabled when commissioning IP capable devices.

The use of network management tools such as SNMP is restricted to IT Services staff, unless requests have been approved.

University servers running Domain Name Service (DNS) are managed and maintained by the Networks and Communications Team within IT Services.

University servers running Dynamic Host Configuration Protocol (DHCP) are managed and maintained by the Networks and Communications Team within IT Services.

University servers running Network Time Protocol (NTP) are managed and maintained by the Networks and Communications Team within IT Services

University servers running RADIUS and TACACS+ are managed and maintained by the Networks and Communications Team within IT Services.

Management interface access

Network appliances and devices shall not expose any management interfaces via the Internet. All management interfaces shall have the appropriate restrictions applied so access is only granted via privileged networks.

Remote access to devices connected to the University’s network is onlt permitted via the VPN.

Only Remote Desktop Protocol (RDP), Virtual Network Computing (VNC) and Secure Shell (SSH) protocols are permitted through the VPN as standard. If other protocols are required for management and/or service delivery, please contact IT Services to discuss your requirements.

Incidents and emergency procedures

Any incident or emergency relating to the University's network should be reported to the Service Desk in IT Services.

Members of the Networks and Communication Team must immediately report any information security incidents to the IT Security Team.

IT Services must ensure that prompt and effective action is taken in response to requests and information from Jisc CSIRT (Computer Security and Incident Response Team).

5. System Management

Purpose

The University's information systems are a fundamental resource for the University and its business. It is vital that such a resource is properly controlled, maintained and managed. This section covers the management, operation and use of University Information Systems.

This sub policy covers all computers owned or operated by Loughborough University and any computers that are present on the campus network which are connected under the agreed Business and Community Engagement Jisc Policies.

Policy

The University's Information Systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve data security, confidentiality, integrity, availability.

All systems management staff shall be given relevant training in information security and sufficient training to securely operate the systems they are required to manage.

System management staff will undertake their duties in collaboration with Technical Service Owners and subject matter experts whose services are running on these Information Systems.

System management staff and Technical Service Owners should deploy systems to agreed secure baselines (systems will be hardened, this may include hardware, network applications and Operating System hardening methods) Secure baselines will be agreed with the IT Security Team.

Information systems must deploy and install all updates and security patches for Operating systems and applications within 14 days of the updates/patches being released

Technical Service Owners or individuals responsible for Information Systems are to maintain the appropriate access controls for their systems and keep records of any elevated access they give out to other users.

Technical Service Owners or individuals responsible for Information Systems are responsible for correct and secure operation of computers in accordance with related University policies.

Access to all Information Systems, excluding publicly accessible data sources, shall use a secure authentication process which incorporates multi-factor authentication. Consideration should also be given as to whether it is appropriate and feasible to further limit the access to business-critical systems by time of day, the location of the access, or by an automatic timeout following a defined period of inactivity. Access to information systems is to be centrally logged and monitored where appropriate to identify potential misuse of systems or information.

Administrator accounts and accounts with elevated privileges must only be used, when necessary, in order to undertake specific tasks which require the use of these accounts. At all other times, the principle of 'least privilege' should be followed.

Browsing internet resources of accessing emails is strictly prohibited from Information systems and when logged in with an administrator account and accounts with elevated privileges.

All Information Systems will be subject to regular vulnerability scanning (monthly). These scans will be undertaken by the IT Security Team or by approved external assessors.

System Management staff and Technical Service Owners must immediately report any information security incidents to the IT Security Team.

Information Owners, Technical Service Owners, and individuals responsible for the Information Systems must ensure that appropriate backup and system recover procedures are in place, dependent upon the accessed level of criticality of the information concerned. Backup of the University's information systems and critical assets and the ability to recover then is an important priority.

Business Service Owners are responsible for ensuring that the University's information systems and critical data is frequently backed up and procedures for recovery meet the needs of the business.

Passwords for the systems and any privileged accounts should adhere to the University password policy: https://www.lboro.ac.uk/services/it/staff/user-account/password

Storage of passwords should be carried out in accordance with a well-defined password storage policy.

Only authorised staff will be permitted to perform systems administration or management functions. Use of commands to perform these functions should be centrally logged and monitored where it is considered appropriate and feasible to do so.

Formal change control procedures, with audit trails, shall be used for all changes to business-critical systems. All such changes must be risk assessed and authorised by the IT Services Change Advisory Board or relevant manager before being transitioned to the live environment

Security event logs, operational audit logs and error logs must be reviewed on a regular basis and managed by qualified staff.

System clocks should all be synchronised to the Universities NTP server. In the case of computers in the Active Directory this will happen automatically.

6. Vulnerability Management

Purpose

The purpose of this section is to allow IT Services within Loughborough University to scan devices attached to the university network misconfigurations and for vulnerabilities. This is to assist in maintaining a secure and reliable infrastructure.

Vulnerability scanning may be conducted to:

- Identify compromised systems within the campus network;
- Identify virus infected machines within the campus network;
- Identify poorly configured and potentially vulnerable systems attached to the campus network;
- Any device requesting a firewall rule;
- Investigate possible security incidents to ensure systems conform to Loughborough University's security policies.

This sub policy covers all computers, mobiles, tablets, and communications devices owned or operated by Loughborough University and any computers, mobiles, and tablets, or communications devices that are present on the campus network which are connected by Partner Organisations under the Janet Network Connection Policy. This is highlighted in the University AUP.

Scanning

Loughborough University IT Services will use security-scanning software to conduct vulnerability scanning and audit reports.

A number of tools will be used for vulnerability scanning and the tool set will be reviewed annually. This includes Open-Source software, commercial packages and approved external assessors.

These tools will perform the following tasks:

- Host Discovery – identifying computers listening on the campus network;
- Port Scanning;
- Operating System Detection – remotely determine the OS (Windows, Apple macOS, Linux, Apple iOS, and Android;
- Software Version Detection – Interrogating listening services to determine application names and versions;
- Network based infrastructure vulnerability scanning;
- Operating systems security patch audits (Windows, Apple macOS, Linux, Apple iOS, and Android;
- Configuration audit;
- Web application vulnerability testing;
- SQL database vulnerability and configuration auditing;
- Password auditing, checking for default or blank passwords;
- Anti-Virus audit, checking out-of-date virus signatures and configuration errors.

Policy

In an effort to reduce IT Security risks and supplement existing security practices, IT Services will perform regular vulnerability audits on devices connected to the campus network.

IT Services may also scan for vulnerabilities, which are currently being exploited in the wild.

Vulnerability audits will consist of campus network scans for:

- Open communications ports;
- Host operating system detection;
- Host operating system patch levels;
- Remote applications to identify known vulnerabilities or high-risk system weaknesses.

Any new systems or services must have passed a vulnerability scan before being connected to the production network.

Any systems or services, which require off-campus access, are subject to a vulnerability scan before access is granted and throughout the lifetime of the system or service. This is to ensure that the hosts meet and maintains an adequate posture.

All systems or services which currently have off-campus access enabled are subject to vulnerability scanning every month.

Any systems or services that require access via the VPN service are subject to passing a vulnerability scan.

Vulnerability scanning will not search the contents of personal electronic files located on the system.

Scans should not cause disruption to the campus network or services hosted on systems being scanned. Device log files may reflect the scan that takes place.

Servers hosted within IT Services datacentres, will be subject to monthly automated authenticated security scan; and as such will require a service account to have local administrator permissions. If a software firewall is installed, a rule will be required to allow the scanning server's IP address(es).

Servers not hosted within IT Services datacentres, but have services exposed to the Internet are also subject to monthly automated security scan.

Managing Vulnerabilities

Vulnerabilities identified against hosts will be emailed to the Technical Service Owners or individuals responsible for the Information Systems.

Technical Service Owners or individuals responsible for the information systems are responsible for ensuring the identified vulnerabilities are remediated in a timely manner, typically 14 days from release, but dependant on a risk assessment).

Vulnerability remediation matrix

Information Category	Critical Vulnerability	High risk vulnerability	Medium risk vulnerability	Low risk vulnerability
Highly confidential	**Remediate**	**Remediate**	**Remediate**	**Remediate**
Confidential	**Remediate**	**Remediate**	**Remediate**	**Recommended**
Not Sensitive / Public	**Remediate**	**Remediate**	**Recommended**	**Recommended**

The IT Security team will be made aware of identified vulnerabilities which have not been resolved by the Technical Service Owner or individuals responsible for the information system.

If identified vulnerabilities are unable to be resolved, steps must be taken by the Technical Service Owner or individuals responsible for the information systems to mitigate the risk of exposure and ensure the risk is recorded and accepted.

Failure to remediate identified vulnerabilities within a suitable timeframe, typically 14 days from release, may results in firewall rules being removed or removing the network connection from the server. This is to ensure that the security and integrity of the network is not compromised for other information systems and the users of the network.

7. Software Management

IT Colleagues should be fully aware and compliant with the University Software Policy:

http://www.lboro.ac.uk/services/it/about/policies/software/

8. Encryption (Cryptography)

Purpose

This section sets out principles and expectations about when and how encryption of University digital information should (or should not) be used and applies to the following:

- Managers who are responsible for the provision of information systems;
- Staff and students at the University who handle sensitive information through employment or study;
- Third parties who handle sensitive information on behalf of the University.

Use of encryption

Loss, theft, or unauthorised disclosure of sensitive information could be detrimental to the University, its staff or students. Such information includes personal data defined by the UK GDPR and Data Protection Act 2018. Where the University is handling digital personal data that cannot be secured by physical controls, the data must be encrypted.

Data, which must be handled securely, using encryption includes:

- Any personal data classed as sensitive “special category” by the UK GDPR;
- Any data, that is not in the public domain, about a significant number of identifiable individuals;
- Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information;
- Data classified as Confidential or Highly Confidential by the University Categories and Control policy. https://www.lboro.ac.uk/services/registry/information-governance/policy3/

Data described above must be encrypted:

- When stored on a computing device (laptops, mobiles, and tablets) or any computer storage (cloud storage, network shares databases, and spreadsheets) which may be exposed to a significant risk of being lost or stolen. Any device when outside a secure University location should be considered to be at risk, including personal devices;
- Where it is to be transmitted via a computer network using mechanisms that do not incorporate encryption. This could refer to: sending data by email either within or outside the organisation, transferring files offsite, remotely accessing files or web pages;
- Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.

Data being handled by the University is subject to an agreement with an external organisation specifying the use of encryption.

Personal data is to be encrypted and no overriding requirements (from external body) apply, the recommended minimum University standards (or better) must be applied.

University web transactions that involve the transfer of sensitive data or funds must use encryption, e.g. use of HTTPS.

Management of encryption keys

Procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will become neither unrecoverable nor accessible by an unauthorised person;
- To facilitate authorised persons of the University to obtain prompt access to the encrypted information in the case of an emergency or investigation;
- To ensure that encryption keys are always stored and communicated securely;
- To record who holds encryption keys relating to important information;
- To revoke encryption keys when key holders leave.

Where practical, an unencrypted backup copy of critical University data should be securely maintained. Critical backup data should be stored where there is appropriate physical security.

Unsupported use of encryption

Staff and students should:

- Not store encrypted data on University systems except where they are able to justify doing so for legitimate purposes;
- Be aware that the University reserves the right to request, at any time, a decrypted view of the data stored on its systems as well as the option to remove any data.

UK Law and travelling abroad

Upon leaving or entering the UK, you may be required by UK authorities to decrypt any device, or files you have stored on devices in your possession. Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes provision whereby certain public authorities (including, but not limited to law enforcement agencies) can require the decryption of devices or files. Failure to comply with such lawful requests is a criminal offence in the UK.

Similarly, government agencies operating outside of the UK may require you to decrypt your devices or files upon entry to or exit from their territories. If you travel abroad with encrypted data classified as confidential or above, there is a risk that the data may require decryption and therefore a risk of disclosure. It is advised that you consider the consequences of such disclosure and wherever possible information classified as confidential or above should not be taken with you while travelling.

For access to information classified as confidential or above abroad, it is recommended the data remains stored on university systems, with access to the data provided by the University's VPN Service.

Particular attention should be paid to the possible inadvertent export of data subject to UK Data Protection legislation to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling.

Cryptography implementation

All encryption products, standards and procedures used to protect sensitive University data must be ones which have received a public review and have been proven to work effectively. Any product used must be certified to FIPS 140-2.