UNIVERSITY OF LIVERPOOL

IT Services

Infrastructure Management Code of Practice V1.1

Valid from Dec 2023

Business Owner:

Mike Parkins, Head of IT Security, IT Services

Document Author:

James Tickle, IT Security Team Leader, IT Services

Contents

1.0 Purpose

The purpose of this *Code of Practice* is to outline the requirements for securely managing infrastructure within the University – minimising vulnerabilities that put University data and systems at risk of cyber-attack, compromise, and loss. This document outlines the technical security baseline requirements, based on the University Information Security Policy and regulatory requirements including: Data Protection Act 2018, Cyber Essentials certification, National Cyber Security Centre and JISC security policy and guidance; as well as the requirements of our collaboration partners.

Accountable owners

Section 3.2 of this document outlines ownership roles. The Business Owner identified in this section is accountable for ensuring that the requirements detailed in this Code of Practice are implemented. Where responsibility for implementing a requirement is fulfilled by another (for example, by IT Services or a 3rd party), the Business Owner remains accountable for ensuring that the requirement is implemented.

2.0 Scope and Approach

2.1 Scope

This *Code of Practice* is for anyone who owns or runs IT systems within the University whether provided and managed by IT Services or sourced and managed independently by departments. It applies to the following infrastructure:

- Servers (both physical and virtual servers).
- Shared devices (see description below).
- Network Attached Storage (NAS) devices.
- Networking equipment (e.g., switches, routers, firewalls etc.).

The guidance issued in this document is consistent with the requirements of running cloud services, however cloud services are not explicitly within the scope of this *Code of Practice*.

Shared devices

The University environment differs from typical enterprise IT environments in that it is common for computing devices to be used for dedicated, bespoke purposes which cannot easily be classified using traditional IT nomenclature. For example, a computer connected to a piece of lab equipment, shared by many users may be regarded by IT professionals as behaving like a server, however the users of the equipment would be unlikely to view it that way. For ease of distinction, the category 'shared devices' is included within the scope of this *Code of Practice* as a broad term to describe such use cases. The following are illustrative examples (though there are many more):

- Computers connected to or integrated with lab equipment.
- Computers running experiments over long periods, accessed by multiple people.
- Computers running specialist software, accessed by multiple people.

As a rule of thumb, any device accessed by more than one person for a specific purpose should be regarded as a shared device under this definition. This applies regardless of the operating system of the device, and desktop variants of Windows, Mac and Linux should be considered 'shared devices' if they align to the definition above.

2.2 Approach

The *Code of Practice* seeks to define the following:

- Security Principles underpinning effective IT infrastructure management.
- Protection measures that Business Owners and System Owners/System Administrators should apply to protect their information and the University environment.
- Security and support from IT Services that helps achieve the principles of effective IT infrastructure management.

3.0 Security Principles: Know what you have, protect it, govern and review it

Effective management relies on the principles of ownership, inventory management, risk management (by Departmental owners and IT Services) and regular maintenance and review.

3.1 Inventory

Inventory of IT assets connected to the network is recorded and kept, including all infrastructure and devices whether procured, deployed and managed locally or centrally. The asset inventory will help IT Services to work with Business Owners to build in reviews and risk management to establish and maintain a secure operating environment.

3.2 Ownership

Ownership refers to the operational accountability for the service or function that the infrastructure creates or supports (as per Information Security Policy). The following are key ownership roles:

- **Business Owner:** The senior person responsible and accountable for the service (e.g. Dean, Head of Department, Principal Investigator etc.).
- **System Owner/Administrator:** Role in charge of and responsible for managing the systems which provide the service. This includes implementing baseline technical security measures.

Ownership responsibilities are detailed in section 4.0 of this document, and a distribution of responsibilities between Owners and IT Services is outlined in the Infrastructure Shared Responsibilities Matrix.

3.3 Protection measures

These represent the baseline technical security measures the Business Owner and System Owner/Administrator should implement, as outlined in section 4.0. Centralised support, monitoring and incident response are available from IT Services, as described in section 5.0.

3.4 Governance and review

This involves a process of regular review of the IT asset inventory to ensure it is accurate and reliable, and that any changes or updates to infrastructure are reflected in inventory. Only IT assets which have an ongoing business justification should remain in operation. The business justification of infrastructure within the estate should be reviewed annually and revalidated by owners. IT and network devices which are no longer needed should be identified by this process and decommissioned through to secure disposal in a timely manner.

4.0 Technical Protection responsibilities for Business & System Owners

This section outlines technical security controls which constitute the baseline minimum protection measures which should be implemented by Business Owners and System Owners/Administrators. A description of each control is given in the left-hand column, while specific ownership responsibilities are listed on the right.

Technical security Control area	Business Owner and System Owner responsibilities
Infrastructure registration and IT asset inventory Capturing the owner and responsible roles. Description of data and sensitivity / data classification. May include: contractual / regulatory requirements e.g., Cyber Essentials, NHS DSPT, GDPR, PCI DSS etc. Whether external, off-campus connectivity is required.	• Complete Infrastructure registration and annual review / revalidation of your IT asset inventory entries. • Notify IT Services of the transfer in ownership or other registered details of any IT assets. • Discuss requirements for data centre hosting as per IT Services New Hardware and Data Centre Hosting Policy • Work with IT Services to identify and prioritise security controls (technical and organisational) in accordance with legislative, regulatory, and contractual requirements. For specific technical controls, such as encryption, please outline and discuss requirements with IT Services Business Partnering, to enable assessment. • Owners should engage with relevant University teams for specific advice, e.g., Records Management for Retention advice, Data Protection advice etc. • Use IT Services contracted IT asset disposal partner for secure erasure and disposal of all data bearing IT equipment (as per Section 2.1 Scope)
Patching / Vulnerability management Suppliers release periodic updates (patches) to operating systems and applications to resolve bugs and security vulnerabilities. Failure to fund and maintain operating system, application and software patches increase a device's vulnerability to attack, which increases vulnerability of the University network as a whole. Patches flagged as '*critical*', or '*security*' updates should be installed without delay.	• Monitor the release schedules of updates to the firmware, operating systems and applications which run on any infrastructure you own. • Assess impact of installing the update. • Speak to IT Services for advice and to develop a risk management plan when standard patching and updates may not be feasible.

Security Device level controls and actions which provide layers of defence against threats. Device level controls include tooling, such as: anti-malware and Security Information and Event management (SIEM) tools, which detect, report and mitigate threats, overseen by the IT Security Team. Encryption and SSL certificates which protect data confidentiality and integrity. Secure web application delivery via Web Application Firewalls (WAF) which provide protection against attacks which target web applications. Actions include responding to threats or vulnerabilities identified by the IT Security Team and securely configuring owned infrastructure and applications to ensure they do not expose undue risk.	• Ensure the University, centrally managed, anti-malware is installed on their devices. • Ensure that SIEM agent software is installed and reporting into the Security Operations Centre (SOC). • Ensure SSL certificates are applied and maintained. • Discuss Encryption requirements with IT Services via the Business Partnering contacts (see above). • Ensure web applications are delivered via the Application Delivery Controller (ADC) and that Web Application Firewalls (WAF) are configured. • Respond to security alerts which are generated by security tools or the IT Security Team. • Ensure that vulnerabilities are resolved within required timescales. • Configure all systems to use the University's NTP servers for time synchronisation. This is required to make sure consistent timestamps for events across all logs regardless of the system that generated them.
Network and firewall Connectivity In order to protect the University network as a whole it is essential to monitor and record connections which are permitted in and out of the campus infrastructure, including internet connections. This is managed by network security infrastructure including firewalls which block or allow connections based on rules. This includes the following controls: • Security review of requests for new external connectivity • Assigning ownership of firewall rules which permit external connectivity. • Review and revalidation of firewall rules on an annual basis. • Disabling firewall rules allowing access which is no longer needed.	• Complete the Infrastructure registration process to update IT asset inventory, and Firewall Rule request. • Don't put anything on the network until it has been reviewed by the Technical Security team. • Work with IT Services to manage the security risks of connections to any infrastructure you own. • Ensure audit logs of inbound access to owned services (firewall rules) are maintained with accompanying business cases. • Review and revalidate firewall rules on an annual basis. • Notify IT Services (via a Service Desk ticket) when firewall rules are no longer required.
Access Management and passwords Access management defines the measures taken to enable access to infrastructure and services and to ensure that this is restricted to those with a legitimate business purpose, that access is the minimum level necessary, is regularly reviewed and removed when no longer necessary. Password controls, including complexity rules and changing of default	• Validate business need of user accounts prior to granting access. • Apply the principle of 'minimum privilege' at all times. • Review accounts regularly and disable when no longer required. • Apply password management to align with University user accounts password policy: ○ Change default 'out of the box' passwords ○ Enforce password complexity

passwords are minimum requirements. Discuss use of IT services centrally provided Multifactor authentication	○ Do not share passwords ○ Reset passwords when requested to do so by IT Services (e.g., following a security incident)
Backup Backup of data provides a means to restore the state of a service in the event of a serious incident which results in the loss of data held on a device. A backup strategy should consider the frequency that backups are taken, the media that data is backed up to and the location in which backed up data is held. IT Services can provide advice and recommendations on suitable backup strategies.	• Determining the backup requirements of any infrastructure you own. • Implementing suitable backup arrangements to meet requirements. • Ensure backup infrastructure is maintained. • Ensuring that systems can be successfully restored from backup when required. • Discuss and request advice from IT Services as required.
Resilience/availability requirements Resilience addresses maintaining service in the event of infrastructure failing or going offline. This includes powering devices and whether resilient power options such as a UPS (Uninterruptible Power Source) are required. Common approaches include: **High availability (HA):** Where multiple devices share the load of providing service. **Hot standby:** Where a second device automatically takes over in the event of a failure. **Warm/cold standby:** Where a second device can be manually enabled to take over. **No resilience:** Where the service becomes unavailable if the infrastructure fails. IT Services can help advise you on resilience and best practice for given services and deployments.	• Determining the level of resilience required for any infrastructure you own. • Implementing the desired level of resilience.* • Managing the risk associated with any outage on their infrastructure. • Request advice from and discuss with IT Services the resilience options and good practice for given services and deployments. *IT Services provided infrastructure has a default level of resilience included – owners should ensure this is sufficient for their needs
Supplier Management Services which run on infrastructure in the estate may incorporate the services, software or infrastructure of 3rd parties as part of their design. Before procuring infrastructure or services from suppliers, IT Services reviews the security practices and accreditation of the supplier and their product – to inform purchasing decisions from a security perspective and to identify any potential security risk associated. IT Services should be	• Ensuring that a Supplier Security Questionnaire has been completed by the supplier and reviewed by IT Services. • Managing any security risk identified in 3rd party provided services. • Maintaining the relationship with 3rd party suppliers. • Ensuring that appropriate maintenance arrangements are in place with 3rd party suppliers.

engaged to review a Supplier Security Questionnaire (SSQ) BEFORE making any commitment to purchase. Where 3rd party services are provided, the role of maintaining services and infrastructure is usually held by the 3rd parties themselves and not University personnel. Where this is the case, owners should maintain relationships with those 3rd parties and ensure that any maintenance obligations are fulfilled as required.	• Ensuring that maintenance obligations (including patching) are completed as required by the service. • Request guidance from IT Services on appropriate technical expectations of 3rd party suppliers.

5.0 Security & Support from IT Services

IT Services holds overall responsibility for the delivery and management of centralised IT services within the institution. IT Services has several specialist teams with different responsibilities in respect of infrastructure management – including the Systems, Network Services, and IT Security teams. IT Services responsibilities include the following:

- Carrying out vulnerability scans to identify any known vulnerabilities present within network connected assets (server/NAS etc) which need remediation.
- Receiving, coordinating, and supporting the University-wide responses to security alerts.
- Managing the Security Operations Centre (SOC), including receiving, triaging, and responding to security issues reported by University personnel.
- Conducting security reviews of new requests for firewall rules and network connections.
- Maintaining inventory and business justification of firewall rules enabling inbound connections across the University perimeter firewalls.
- Monitoring infrastructure inventory. Investigating and taking action if technical protection or ownership details are insufficient, or if the business justification is not validated.
- Deploying and configuring server software on managed servers, including security software, remote management software etc.
- Deploying and managing the Security Information and Event Management (SIEM) capabilities, including (but not limited to):
    - Monitoring for anomalous user access attempts which may indicate a cyber threat.
    - Receiving, correlating, and analysing server logs to detect potential cyber threats.
    - Ensuring that servers have appropriate technical security tooling installed.
- Maintaining backup infrastructure and performing restoration from backup as required (for services using the centralised University backup service).
- Ensuring systems can be restored from backup as required (for services using IT Services infrastructure).
- Providing a default level of resilience for services using IT Services infrastructure.
- Supporting Business and System Owners with advice and responding to support requests on the technical protection measures outlined in section 4.0, above.
- Provision of IT Services contracted IT asset disposal partner for secure erasure and disposal in line with Waste Electrical and Electronic Equipment (WEEE) Regulations.

Compliance and Security incident response

The cyber security threat landscape creates day to day operational management challenges which often require a rapid, coordinated response to ensure that University systems and data are not compromised and remain available for their intended purpose. This often involves University-wide remedial action with IT Services in response to known threats, including:

- Liaising with law enforcement, the National Cyber Security Centre, intelligence partners and University leadership to understand the threat and its potential impact on the University.
- Notifying affected Owners and stakeholders of the details of the threat.

- Assessing impact to the University network and services, including remediation plans. This may include temporary disconnection of services as per the IT Acceptable Use Policy.
- Monitoring and reporting on the progress of remediation plans to Senior management.
- Supporting Owners and other stakeholders with the detail of remediation or any queries relating to security threats.

6.0 Monitoring and Compliance

Owners and Administrators are urged to implement the controls described in this document as fully as practicable and demonstrate a disciplined risk management approach when controls cannot be implemented. IT Services will take reasonable steps to measure compliance with controls for all infrastructure on the network. Where infrastructure fails to meet security best practices, IT Services will work with owners to help remediate issues – reporting any persistent or serious security failings to Senior Leadership.

Where it is not possible to secure infrastructure or reduce the associated risk to a tolerable level, IT Services reserves the right to disconnect such devices from the network, until appropriate mitigation can be put in place.

7.0 Document control

Document Version Control			
Author	**Summary of changes**	**Version**	**Approval (Role & date)**
Jimmy Tickle – Senior Security Analyst	Initial issue	1.0	Mark Hilditch, Head of Infrastructure & Operations, 22 July 2021
Jimmy Tickle – Senior Security Analyst	Moderate revision, including: Scope widened to apply to all infrastructure (previously just servers). More definition added to define devices in scope and ownership responsibilities. Additional protection measures and IT Services responsibilities added to align to Responsibilities matrix and Supplier Security Questionnaire.	1.1	IT Services SMT: 16/11/2023
Policy Ownership & Review			
Owner and contact for enquiries	This document is owned by the Associate Director for Service & Infrastructure of the IT Services department. The IT Security team are the document authors and initial point of contact for any enquiries, via email at itsec@liverpool.ac.uk.		
Review due:	13Nov 2024		
Document location	https://www.liverpool.ac.uk/it/regulations/		
** Owner & Author are responsible for communicating this document**			