Network Management Code of Practice

Executive Summary

The University's IT network is a critical asset that supports the university's academic, administrative, and research activities. Ensuring its security, integrity, and availability is paramount to maintaining the trust of students, staff, and stakeholders.

The CoP outlines the responsibilities of network management staff, the procedures for network design and configuration, and the measures for physical and logical security. It also addresses the processes for change management, incident response, and compliance monitoring. By following this CoP, the university aims to create a secure and resilient network environment that supports its mission and objectives.

These requirements must be adhered to by all users to;

- ensure that the University complies with its legal and statutory obligations,
- protect the confidentiality, integrity and availability of information and systems, and
- provide authorised users of university IT with a safe and acceptable working environment.

CoP Statement

1. The university is committed to maintaining the highest standards of information security and operational resilience. This CoP will define how the University networks are designed and how IT systems, services and devices are connected to them.

2. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of the wider IT Security CoP set.

3. By adhering to these standards, the university demonstrates its commitment to maintaining a robust information security posture and safeguarding sensitive data.

Purpose

4. The purpose of this Network Management CoP is to establish a framework for the secure and efficient management of the university's network infrastructure.

5. Unless explicitly stated otherwise in this CoP, the JANET Acceptable Use Policy applies to all users of the University IT systems and services.

Scope and Application

6. This CoP applies to all staff employed by the University and authorised users that have access to information and information technology provided by or through Leeds Beckett University.

7. It applies to all facets of the University IT Environment.

8. All applicable users are required to familiarise themselves with this CoP and comply with its requirements.

9. Failure of university users to comply with this CoP may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

10. Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action.

11. Completion of the University's Cyber Security Training module is required by all users to support the effective implementation of this CoP.

Standards

12. Use of the University IT Environment is subject to law and regulation, and the University seeks to ensure compliance with these via this CoP.

13. The CoP also supports adherence to standards required for University PCI DSS accreditation (this being the technical and operational requirements for processing credit card data) and Cyber Essentials (this being a standard for information security).

DEFINITIONS

14. University IT Environment - includes all servers and clients, network connectivity, systems and application software, internal and external services, data, and other computer subsystems and components that are owned or provided by the University, or which are under the University's responsibility.

15. Software Patch - a piece of code designed to update, fix, or improve a computer program or its supporting data.

16. Assets – Any valuable resource that needs protection from compromise or potential attack. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., data, information, software, patent, or intellectual property)

17. User – any individual afforded access to the University IT Environment via a direct relationship with the university, including Students, Staff and Associated persons or body's

18. Student - Any individual enrolled on a Leeds Beckett University programme of study, including apprentices registered on University's degree apprenticeship programmes and those at partner institutions registered as LBU students.

19. Staff - Any individual on a contract of employment including officers, employees (whether permanent, fixed term or temporary), workers, trainees, seconded staff, agency staff, volunteers, interns or any other person working in any context within the University.

20. Associated person or body - Any person or body engaged on University business by which we mean individuals performing or providing services for or on behalf of the University which may include governors, University subsidiaries, contractors, recipients of grants, partners, collaborative arrangements, joint ventures, agents and advisors etc. For the purposes of the CoP, this also includes any third parties representing Leeds Beckett.

21. Malware - a piece of computer code, most often a malicious software program designed to destroy or damage information on computers. Some viruses cause no damage apart from reproducing, but a significant number are specifically designed to cause data loss or to compromise the confidentiality of files by sending copies of them to others.

    Potential sources of viruses include external storage media such as USB sticks or hard-drive, e-mail attachments, software or digital documents copied over networks, and malicious links, files or website traffic transferred over the Internet.

22. End User Network Device – any network enabled device which is the initial source or ultimate destination in a data network.

23. Network Device – a device such as a switch, router, load balancer or firewall through which data passes on its journey to or from an End User Network Device.

24. Network Interface – part of a network device or end user network device that enables it to communicate via a network, there may be more than one interface on a device.

25. Local Area Network (LAN) – a computer network that spans a relatively small area, such as a building.

26. Network Manager – The person appointed by the University as the person responsible for the management of the University network.

27. System Owner – The manager of individual systems or services such as email or websites. Can include PC labs or LAN partitions.

RESPONSIBILITIES

Responsibilities and application of the CoP

28. The Vice Chancellor is responsible for ensuring that the CoP is implemented and maintained, and for ensuring all necessary resources are available to support this.

29. The Director of Digital Services is responsible for operational coordination of the CoP.

30. The Director of Digital Services is responsible for ensuring appropriate policies, procedures, guidance, advice, and training are in place to support the CoP's implementation and compliance, and for ensuring these artifacts are regularly reviewed at appropriate intervals.

References and Associated Documentation (Legislation, Other Policies, other parties)

31. This CoP forms part of a suite of related Information Security policies.

OPERATIONAL APPLICATION

Management of the Network

32. The University's network shall be managed by suitably authorised and qualified staff appointed by the Director of Digital Services.

33. Appointed staff will oversee the day to day running of the network and preserve its security and integrity in collaboration with nominated individual system owners.

34. Authorised staff and third parties who necessarily have appropriate privileged access to critical infrastructure must understand and comply with the university's information security policies.

35. Any network-related security incidents must be reported immediately to the through the university's incident reporting process, with the internal university C-SIRT (Computer Security Incident Response Team) being made aware as a matter of priority.

36. Authorised staff must act promptly to protect the security of the network but must also be proportionate in the actions that they take, particularly when undertaking actions that have a direct impact on the users of the network.

37. Where there is a risk to the security or quality of service to the network the Network Services manager is authorised to make emergency changes to restore service.

38. Any actions that may potentially be invasive of users reasonable expectations of privacy must be undertaken in accordance with instructions approved by the University's Data Protection Officer (or their nominee).

39. Any planned reconfiguration of the network must go through formal, auditable change control procedures and an appropriate level of risk assessment and management.

40. Overall control of the IP address scheme is managed by the Network Services manager, although this may be delegated to nominated system owners for limited IP address management.

41. Users of the network must be advised that network management procedures will include procedures such as:

    - Probing devices to test security.

    - Monitoring of network traffic to detect operational issues.

    - Recording of network traffic to detect possible CoP violations.

    - Validation that data travelling across the network is legitimate and does not have malicious content, is not of an offensive nature, and cannot be detrimental to performance or management of any device or end user device on the network.

    - Monitoring, filtering and blocking of websites and other services where necessary to protect against malicious cyber attacks and fulfil the University's statutory and regulatory responsibilities.

Network Design and Configuration

42. The network must be designed and configured to deliver a level of performance, reliability and security suitable for the requirements of the university, whilst providing a high degree of control over access to the network.

43. The network must be segregated into separate logical domains with routing and access controls operating between the domains to prevent unauthorised access to network resources, critical business systems, and unnecessary traffic flows between the domains.

44. Network configurations must be approved by the university's TDA (Technical Design Authority).

45. Regular reviews and updates to network design must be conducted to meet evolving business needs.

46. LANs in individual buildings or departments should normally be designed and installed by the network management team. In other cases, the Network Services manager reserves the right to check the installation before connecting it to the University's core network.

47. Any device that is running a service that conflicts with centrally managed services must not be connected to the network without prior agreement with the university's TDA or DSLT (Digital Services Leadership Team).

48. No changes to the network infrastructure, such as the introduction of a router, switch or wireless access point, is permitted without prior approval from the Network Services manager.

49. Records of all active and inactive network device locations and configurations shall be maintained.

Physical Security and Integrity

50. Reasonable measures must be taken to protect rooms containing servers, active network devices and patching panels from threats such as fire, water, accidental damage, security breaches and theft. The selection of these measures should be based on a risk assessment that takes into account the need for regulatory compliance.

51. Access to these facilities must be restricted to authorized personnel only.

52. A list of authorised staff must be maintained by the relevant system or Network Services manager.

53. Other individuals must only be provided access once their entry has been approved by the relevant system or Network Services manager.

54. The network should be resilient to help mitigate the impact of the failure of network components.

55. Any device that is running a service that conflicts with centrally managed services such as OSPF, DHCP, RIP, BOOTP etc. must not be connected to the network without prior agreement with the Network Services manager.

Change Management

56. All changes to network infrastructure must follow a formal change management process.

57. Changes must be documented, reviewed, and approved by relevant stakeholders before implementation.

58. A record of the configuration of all network devices will be kept, and any changes to the network device configuration recorded in accordance with Digital Services Change Control processes.

Capacity Management

59. For future capacity planning, Information Services will monitor and record levels of network traffic capacity throughout the network infrastructure.

Connecting Devices to the Network

60. Only authorized devices may connect to the wired university network. Exceptions must be approved by the Network Services manager.

61. Partner/3rd party access to the network shall be based on a formal contract that satisfies all necessary security conditions.

62. It is not permitted to connect personally owned equipment to any network socket that has not been provided specifically for the purpose.

63. It is permissible to connect personally owned equipment to appropriate University provided wireless networks.

64. Any device connected to the University network must be managed effectively and conform to University requirements and policies. Devices are liable to physical or logical disconnection from the network without notice if not.

65. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal operational practices.

Network Address Management

66. IP address allocation and management must be controlled to prevent unauthorized access.

67. Network addresses assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

68. Regular audits of IP address usage must be conducted.

Network Boundary Management

69. Firewalls and other boundary protection devices and services must be configured to prevent unauthorized access and protect against malicious activity and cyber attacks.

70. Regular reviews and updates to boundary protection measures must be conducted.

Access Controls

71. Access to network resources must be strictly controlled to prevent unauthorised access.

72. Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

73. Digital Services are responsible for the management of gateways that link the university's network to the Internet. Controls will be enforced at these gateways to limit the exposure of University systems to the Internet to reduce the risks of hacking, denial of service attacks, malware infection and propagation, and unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.

74. Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

75. Remote administrative connection to the University network and resources will only be permitted from authorised users and devices over suitably secured connections.

Network Device Configuration

76. There will be documented standards/procedures for configuring network devices which cover:
    - security architecture principles
    - standard security management practices
    - device configuration
    - restricting access to network devices
    - vulnerability and patch management
    - changes to routing tables and settings in network devices
    - regular review of network device configuration and set-up

77. Security controls applied to network devices should incorporate security architecture principles.

78. Network devices should be subject to standard security management practices, which include:
    - restricting physical access to network devices to authorised staff.
    - hardening the operating system(s) that support them.
    - applying a comprehensive set of management tools.
    - keeping network devices up to date.
    - monitoring network devices.

79. Network devices should be configured (typically based on a standard secure build) to:
    - log security-related events in a form suitable for review, and record them on a separate system CoP
    - integrate with access control mechanisms in other devices
    - use a predefined secure set-up upon boot
    - ensure that passwords are not sent in clear text form

80. Access to network devices should be restricted to authorised network staff, using access controls that support individual accountability, and protected from unauthorised access

81. There should be a process for dealing with vulnerabilities in network devices that includes:
    - monitoring them for known vulnerabilities.
    - issuing instructions to network staff on the action to be taken if a network device fails
    - testing patches for network devices and applying them in a timely manner.

82. Network devices that perform routing should be configured to prevent unauthorised or incorrect updates by:
    - verifying the source of routing updates
    - verifying the destination of routing updates.
    - protecting the exchange of routing information.
    - encrypting the routing information being exchanged Network devices should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and to assess activities performed on the network device.

COP MANAGEMENT

CoP Review

83. This CoP will be reviewed every two years. It is the responsibility of the Head of Cyber Security to ensure that these reviews take place and remains internally consistent.

84. Reviews resulting in minor changes shall be signed off by the Director of Digital Services prior to deployment. Substantial changes to the CoP shall be approved by the Digital Services Senior Management Board prior to deployment.

85. Substantive changes to this CoP shall be communicated to all relevant Users.

CoP Specifications

Organisation	Leeds Beckett University
Author(s)	Dominic Jennings (Cyber Security Assurance Analyst)
Developed in consultation with	Digital Services, Cyber Security, Information Governance, Registrar & Secretary's Office
Owner	Director of Digital Services
Target audience	All staff, students and all other relevant parties
Sensitivity	Public

EDI Assessment	The policy supports the principles of the university's approach to IT and Cyber Security and includes a commitment to complying with legal and regulatory requirements by adhering to applicable UK laws and regulations ensuring fair, transparent and equal implementation of controls. No significant EDI impacts have been identified. The CoP will continue to be monitored to ensure fairness, transparency, and equality of treatment for all users
Approved by	Director of Digital Services
Endorsed by	Digital Services Management Board
Effective from	11-04-2026
Last review date	11-04-2026
Next review date	+2 years from last date of approval [04-2028]
Status	**Published**
Distribution	All Services, Staff, Teams, and Users.
External references	None
Links to other internal policies / procedures	University policies | Leeds Beckett University
Version reference	1.0
Version History - summary of changes (inc. committee paper reference if applicable)	New CoP. Supersedes previous CoP/guidance contained in IT Security Policies.