Logging and Monitoring Code of Practice

Executive Summary

The security of information systems is paramount to the success and reputation of the university. Effective logging and monitoring are critical components of the university's information security strategy, enabling the detection, investigation, and response to security incidents.

This CoP outlines the university's commitment to implementing comprehensive logging and monitoring practices to safeguard its information assets.

By adhering to this Logging and Monitoring CoP, the university aims to;

- ensure that the University complies with its legal and statutory obligations,
- protect the confidentiality, integrity and availability of information and systems, and,
- protect the interests of users of university systems and services

CoP Statement

1. Effective logging and monitoring are critical components of the university's information security strategy, enabling the detection, investigation, and response to security incidents.

2. The CoP will help to ensure that the university maintains a clear audit trail of user actions and system events to support accountability and traceability. It will also enable the timely detection and response to security incidents to minimize potential damage and recovery time.

3. This CoP provides information on the circumstances in which it is permissible for the University to access information stored in User Accounts, or to monitor use of IT systems and services including internet use.

Purpose

4. This CoP outlines the requirements for logging and monitoring activities within the university to ensure the security of the University IT Environment.

Scope and Application

5. This CoP applies to all university staff, contractors, and students who use university information systems and networks. It encompasses all forms of data and system activities, including user access, administrative actions, and security events.

6. It applies to any device that may be used to access the University IT Environment, including personally owned devices.

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

8. 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.

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

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

Standards

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

12. 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

13. 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.

14. 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)

15. 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

16. 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.

17. 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.

18. 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.

19. Logging - The process of recording events, transactions, or activities in an information system. Logs provide a record of actions taken by users and systems, which can be used for auditing, troubleshooting, and security purposes.

20. Monitoring -The continuous observation of systems and networks to detect and respond to security incidents, performance issues, and other anomalies. Monitoring helps ensure the ongoing security and availability of information systems.

21. Log Data - Information captured in logs, including details such as the date and time of the event, the user involved, the nature of the event, and the outcome.

22. Real-Time Monitoring - The process of continuously observing systems and networks in real-time to detect and respond to security incidents as they occur.

23. Audit Trail - A chronological record of system activities that provides evidence of user actions and system events. Audit trails are used for accountability, compliance, and forensic analysis.

24. Compliance Monitoring - The process of ensuring that logging and monitoring practices adhere to relevant standards, regulations, and policies.

RESPONSIBILITIES

Responsibilities and application of the CoP

25. 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.

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

27. 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)

28. This CoP forms part of a suite of related Information Security documents.

OPERATIONAL APPLICATION

Logging requirements

29. As a minimum, all critical systems and applications must generate logs that capture key events, including user access, administrative actions, and security events.

30. Logs must include sufficient detail to identify the nature of the event, the user involved, the date and time, and the outcome.

31. Logs must be protected against unauthorized access, modification, and deletion.

32. Logs must be retained for a minimum period as required by legal, regulatory, and business requirements (e.g. one year).

Monitoring requirements

33. Where possible and appropriate, real-time monitoring of critical systems and networks should be implemented to detect and respond to security incidents promptly.

34. Detected incidents must be reported through the university's incident reporting process immediately.

35. Alerts must be configured for significant security events, such as unauthorized access attempts, system failures, and unusual activity.

36. Regular reviews of logs and monitoring data must be conducted to identify potential security issues and ensure compliance with this CoP.

37. Monitoring for routine operational reasons is completed to ensure that IT systems and services are performing properly. This data may be used for data analytics.

38. Monitoring of University IT Environment usage that involves accessing data in user accounts may only be undertaken by specific members of staff as a recognised part of their normal duties.

39. In the event of a security incident authorised staff may investigate which system and/or individual is the source of the incident. Any investigation of this kind must comply with other relevant university policies and procedures.

40. Information generated by the use of devices to access the University IT Environment may be routinely monitored to:
    - Support detection or prevention activities that are in breach of University CoP
    - Comply with legislation
    - Support detection or prevention of activities that are illegal
    - Defend against attacks against its systems or data

- Identify or investigate an operational problem or monitor for correct operation
- Perform monitoring or support activities with consent of the subject
- Investigate suspected unauthorised access to or use of systems

41. User-specific information may be routinely monitored or logged by authorised staff with respect to:
    - Login and logout events and locations
    - System resource usage
    - Internet usage
    - Software usage
    - Software auditing to support compliance
    - Network bandwidth usage and traffic patterns
    - Power consumption
    - Detection of email spam
    - Detecting security vulnerabilities
    - Identifying and controlling security threats
    - Detecting inappropriate content, which may include material, which is obscene, violent, illegal, damaging to the University or otherwise in breach of University CoP.

42. Routine monitoring may make use of automated systems that scan user files and communications for an approved purpose.

43. In special circumstances, such as those mandated by legal or CoP compliance, authorised University staff may access and examine the content of data stored in, or being transmitted by, University IT systems and services. This includes examining the content of files and communications that should otherwise be treated as confidential and therefore goes beyond what is permitted in routine monitoring.

44. Monitoring or access to data for the purposes of legal or CoP compliance may only be carried out with the proper authorisation.

45. Automated tools will be used to scan incoming and outgoing email for spam and malware. Email content is not otherwise routinely monitored.

46. Automated actions, such as diversion to junk-emails folders or discarding of emails, will be taken if malicious or otherwise unwanted elements are identified by these tools prior to delivery to the user's mailbox.

47. Attachments identified as a potential security risk may be removed.

48. All individuals are responsible for ensuring that their internet use is compliant with university policies and the law.

49. The University reserves the right to block access to web sites where it is deemed necessary, for legal or compliance reasons or to protect users of the University for example.

50. The University reserves the right to conduct scans of the network to determine what devices are connected to it and what network services are running on the device.

51. If there are reasonable grounds to believe that a device connected to the network may present a security risk or contravene University policies action may be taken to prevent the device connecting to University resources until the issue is resolved

52. The University will conduct (or commission from third parties) penetration tests or vulnerability scans of the University IT Environment to identify potential security weaknesses.

53. Any monitoring information that is collected in relation to a student or member of staff may be used in a disciplinary investigation, for example where there is inappropriate use of the internet or e-mail.

54. Information collected may also be passed to relevant authorities if there are any criminal proceedings to which it relates.

55. Monitoring information may be used for training purposes, for example telephone training.

56. Monitoring information may also be used for analytical purposes to plan and deliver IT and telecommunications services.

57. The university will provide access to third parties where there is a legal reason for doing so. For example, information may be requested as part of legal proceedings including Freedom of Information Act, Data Protection Act 2018 or Regulation of Investigatory Powers Act.

58. Information gathered during routine monitoring operations will be kept according to the universities Records Retention Schedule.

COP MANAGEMENT

CoP Review

59. 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.

60. 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.

61. 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.