Access Control Code of Practice

Executive Summary

Leeds Beckett University is committed to protecting its IT Environment. To achieve this, the university will implement robust access control measures to regulate and monitor access to its systems, networks, and data.

By enforcing this Access Control Code of Practice (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,
- protects the interests of users of university systems and services

CoP Statement

1. Access to university information systems will be granted based on the principles of least privilege and need-to-know, ensuring that users have the minimum level of access required to perform their duties. All access requests will be subject to approval and regular review to maintain security and compliance with relevant standards and regulations.

2. The university will employ multi-factor authentication, role-based access controls, and regular audits to safeguard its information assets. Users are expected to adhere to this CoP and report any security incidents or unauthorized access attempts immediately.

Purpose

3. The purpose of this CoP is to establish the principles and requirements for controlling access to Leeds Beckett University's information systems and data, ensuring the confidentiality, integrity, and availability of IT Environment.

Scope and Application

4. This CoP applies to all university employees, students, third-party contractors and service providers, and any other individuals who have access to the University IT Environment. This includes users accessing from university premises or from remote locations.

5. This CoP will be provided to all new and existing staff and members of the University who have a responsibility for the development and management of services provided by suppliers.

6. Supplier staff must also be made aware of the CoP where they have a responsibility for ensuring that it is implemented.

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. Privileged Account – A privileged account is a type of user account with more permissions and access rights than a standard account. Privileged accounts allow users to make significant changes to a system, such as changing system configuration, installing software, accessing sensitive data, or creating new user accounts. They may also be known as Administrative or Admin Accounts.

RESPONSIBILITIES

20. The Vice Chancellor is responsible for ensuring that all necessary resources are available to support the implementation of this CoP across the University.

21. The Director of Digital Services is responsible for the operational coordination of the CoP and 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)

22. This CoP forms part of a suite of related Information Security policies that can be found here (insert link).

OPERATIONAL APPLICATION

Access Control Principles

23. Access to information systems and data must be granted based on the principle of least privilege, ensuring users have the minimum level of access necessary to perform their duties.

24. Access to sensitive information must be restricted to individuals who have a legitimate need to know.

25. Access permissions must be assigned based on user roles and responsibilities.

User Access Management

26. A formal process must be followed for granting and revoking access to information systems and data.

27. New users must be registered through a formal process that includes identity verification and approval from the appropriate authority. Access must be promptly revoked when users leave the university or change roles.

28. Access rights must be assigned based on job roles and responsibilities.

29. Access requests must be approved by the user's manager and the information owner. Access rights must be reviewed regularly to ensure they remain appropriate.

30. Generic identities must not be permitted as means of access to University's data. Under all circumstances, users of accounts must be identifiable for the University to meet the conditions as an IT service provider.

31. Strong authentication mechanisms must be implemented to verify the identity of users.

32. Multi-factor authentication (MFA) must be used for accessing sensitive systems and data. Passwords must meet university complexity requirements and be changed regularly according to university CoP.

33. Other access control methods must be implemented where available and appropriate, including but not limited to, firewall rules and IDS/IPS based restrictions.

Privileged Access Management

34. Privileged access must be restricted and managed separately from standard user accounts.

35. Privileged accounts must be used only for administrative tasks and must not be used for day-to-day activities. The allocation of and access to privileged accounts must be tightly controlled and monitored.

36. Privileged accounts must not be provided to users by default.

37. Regular reviews of privileged access must be conducted to ensure appropriateness.

38. Privileged access rights must be reviewed at least quarterly to ensure they are still required and appropriate. Any unnecessary privileges must be revoked immediately.

Access Control for Systems and Applications

39. ACLs must be used to manage access to systems and applications.

40. ACLs must be configured to grant access based on user roles and responsibilities. Regular reviews of ACLs must be conducted to ensure they are up-to-date.

41. Duties must be segregated to reduce the risk of unauthorized or unintentional modification of information.

42. Critical tasks must be divided among multiple individuals to prevent conflicts of interest, reduce the risk of fraud or error, and avoid single points of operational or knowledgebase failure.

Physical Access Control

43. Physical access to facilities housing critical information systems must be controlled.

44. Access to data centers and other sensitive areas must be restricted to authorized personnel only. Access must be granted through key cards, biometric systems, or other secure methods.

45. Lost ID Cards must be reported to the IT Service Desk immediately, who will cancel the card through the access control system. Replacement cards must not be issued until confirmation that a prior card has been cancelled. New cards with the same level of access control will be issued by the IT Service Desk.

46. Visitor access to sensitive areas must be managed, logged and monitored.

47. Visitors must be always escorted and their access must be logged. Temporary access must be granted only when necessary and must be revoked immediately after use.

Monitoring and Logging

48. Access to information systems and data must be logged and monitored.

49. Logs must capture details of user access, including the user ID, time of access, and resources accessed. Logs must be reviewed regularly to detect and respond to unauthorized access.

50. Audit trails must be maintained to provide a record of system and user activities.

51. Audit trails must be protected from tampering and must be retained for a period specified by the university's data retention policy.

Access Control for Third Parties

52. Access for third-party service providers must be managed and controlled.

53. Third-party access must be granted only when necessary and must be subject to the same access control principles as internal users. Contracts with third parties must include security requirements and provisions for monitoring and auditing access.

54. Ensure that any sub-processors engaged by third parties comply with the university's access control requirements.

55. Third parties must obtain prior written consent from the university before engaging any sub-processors. Sub-processors must adhere to the same access control standards and be subject to regular audits.

COP MANAGEMENT

CoP Review

56. 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.

57. Reviews resulting in minor changes shall be signed off by the Director of Digital Services prior to deployment.

58. Substantial changes to the CoP shall be approved by the Digital Services Senior Management Board prior to deployment.

59. 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.	New CoP. Supersedes previous CoP/guidance contained in IT Security Policies.

committee paper reference if applicable)	