Supplier Security Code of Practice

Executive Summary

This Code of Practice (CoP) outlines the requirements for ensuring that services provided by suppliers to support the undertaking of University business are secure.

These requirements must be followed 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. Leeds Beckett University operations rely on IT services provided by third party suppliers. It is essential that these services are secured from end to end in accordance with professional best practice and with statutory, regulatory, and contractual requirements around cyber security.

Purpose

2. This CoP aims to ensure that all suppliers providing goods and services to Leeds Beckett University adhere to cyber security standards that protect the confidentiality, integrity, and availability of university business operations.

Scope and Application

3. This CoP applies to all suppliers and partners who can influence the confidentiality, integrity, and availability of Leeds Beckett University business operations, including as this applies to data, systems, services and assets.

4. It also applies to university staff who are involved in developing or managing relationships with those suppliers and partners.

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

6. 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.

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

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

Standards

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

10. 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

11. 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.

12. 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)

13. University User – any individual afforded access to the University IT Environment via a direct relationship with the university e.g. students, members of staff, academics, associates.

14. 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.

15. 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.

16. 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.

RESPONSIBILITIES

Responsibilities and application of the CoP

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

18. 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)

19. This CoP forms part of a suite of related IT Security documents.

OPERATIONAL APPLICATION

20. Leeds Beckett University is committed to maintaining the highest standards of cyber and information security. The following requirements must be met when establishing or managing services provided by suppliers.

Supplier Selection and Due Diligence

21. A risk assessment of potential suppliers must be conducted to evaluate their security posture. This involves identifying potential risks associated with the supplier, assessing the likelihood and impact of these risks, and determining the supplier's ability to mitigate them.

22. Assurances that suppliers meet the university's security requirements must be sought such that risks identified during the risk assessment process are sufficiently mitigated. Assurances can be supported by demonstrable compliance with security standards such as ISO27001, Cyber Essentials, or Soc 2 Type 2 where possible.

23. Security clauses must be included within contracts or agreements, specifying the supplier's responsibilities for protecting university data. These should clearly outline any security expectations, including data protection measures, incident reporting requirements, and consequences for non-compliance. This ensures that suppliers are legally bound to adhere to the university's security standards.

Access Control

24. Suppliers must be granted the minimum level of access necessary to perform their duties.

25. Access controls should be implemented to ensure that supplier staff only have access to the information and systems they need to perform their tasks. This minimises the risk of unauthorized access and data breaches.

26. Strong authentication mechanisms for supplier access to university systems must be implemented. This includes multi-factor authentication (MFA), strong password policies,

and regular password changes to ensure that only authorized individuals can access applicable systems.

27. Supplier access and activities should be regularly monitored to detect and respond to any unauthorized actions via the use of logging and monitoring tools.

28. Regular audits and reviews should be conducted to identify any suspicious activities or CoP violations.

Data Protection

29. Suppliers must handle university data in accordance with data protection laws and university policies.

30. Suppliers must follow best practices for data handling, including data minimization, secure storage, and proper disposal of data. They must also comply with relevant data protection regulations.

31. Encryption of sensitive data during transmission and storage must be implemented. Ensure that all sensitive data is encrypted both in transit and at rest. This includes using secure communication protocols and strong encryption algorithms.

32. Suppliers must promptly notify the university of any data breaches or security incidents.

33. Suppliers should have a clear incident response plan in place and must inform the university immediately if a data breach occurs. This allows the university to take appropriate action to mitigate the impact.

Technical Security

34. Robust network security measures must be implemented to protect university data. This should include, but is not limited to, the use of firewalls, intrusion detection/prevention systems (IDS/IPS), and secure network architecture to safeguard against unauthorized access and cyber threats.

35. Ensure all relevant endpoints (e.g., laptops, mobile devices) used by suppliers are secured. Reputable and up to date endpoint protection solutions, such as antivirus software and endpoint detection and response (EDR) tools, and device encryption must be implemented.

36. Applications provided by suppliers for the undertaking of university business must be secure. Suppliers must conduct regular security assessments to identify and mitigate application vulnerabilities, including vulnerability scanning and penetration testing.

37. Cloud services provided by suppliers for the undertaking of university business must be secure. Suppliers must implement cloud security best practices, such as data encryption, access controls, and regular security audits of cloud environments.

38. The security of Cloud services should be reviewed against the NCSC's Cloud Security Principles.

39. Suppliers must implement robust backup and recovery procedures, ensuring that data is regularly backed up. A tested disaster recovery plan must be in place to restore data and services in the event of a security incident.

Physical Security

40. Supplier facilities must have adequate physical security controls to protect university data and assets. This includes measures such as access controls, surveillance systems, and security personnel to prevent unauthorized physical access to sensitive areas.

41. Access control measures, such as the use of key cards, biometric scanners, must be implemented to restrict physical access to sensitive areas to ensure that only authorized personnel can gain access.

Incident Management

42. Suppliers must have an incident response plan in place and cooperate with the university during security incidents. The incident response plan should outline the steps to be taken in the event of a security incident, including containment, investigation, and remediation. Suppliers must work closely with the university to resolve incidents.

43. Suppliers must report security incidents to the university within a specified timeframe. Establish clear reporting timelines and procedures for suppliers to follow when a security incident occurs. This ensures timely communication and coordination.

Training and HR Screening

44. All supplier staff must complete, or have completed, mandatory security awareness training before accessing university systems or data. This should include comprehensive training on relevant security policies, threat recognition, and best practices.

45. Training materials must be regularly updated to reflect new threats and changes in policies.

46. Appropriate background checks on supplier staff must have been completed before they are granted access to university systems or data. This could include verification of identity, qualifications, and employment history, criminal background checks, and other relevant screenings to ensure trustworthiness.

47. Ensure that all supplier staff understand their obligations to protect confidential information and the consequences of violating the requirements of a contract or binding agreement.

48. The need for supplier staff to sign an NDA (Non-Disclosure Agreement) to protect university data and intellectual property must be considered.

Compliance and Auditing

49. Staff responsible for the management of supplier services should consider conducting security audits of suppliers to ensure ongoing compliance with university policies and requirements where appropriate. This could involve periodic audits to review the supplier's security practices, identify any gaps, and ensure continuous improvement. Audits can be conducted by internal teams or third-party auditors. If unsure, seek advice from Digital Services.

50. Any non-compliance issues should be addressed promptly and corrective actions taken as necessary.

51. A process for managing non-compliance, including identifying issues, implementing corrective actions, and monitoring progress should be established.

52. Suppliers should be held accountable for meeting security requirements.

Termination of Contract

53. Upon termination of a contract, suppliers must return or securely destroy all university data.

54. Ensure that all university data must be either returned or securely destroyed in accordance with University data protection policies to prevent unauthorized access to data after the contract ends.

55. All supplier access to university data, systems, services and facilities should be revoked immediately, or as soon as is practicable, upon contract termination to prevent unauthorised access.

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

58. 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.