Software Management and Secure Development Code of Practice

Executive Summary

The CoP outlines the responsibilities of all stakeholders, including development teams, procurement teams, IT management, and the broader university community, in maintaining a secure software environment.

Adherence to this CoP will 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 security and integrity of software and information systems are paramount to the success and reputation of Leeds Beckett University. We recognise the critical importance of maintaining a secure and reliable software infrastructure that underpins our academic and administrative functions, and of safeguarding our information assets against evolving cyber threats.

Purpose

2. The purpose of this CoP is to establish a comprehensive framework for the secure development, procurement, management, and maintenance of software at Leeds Beckett University.

3. 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

4. This CoP applies to all staff, students, contractors, and third-party partners involved in the development, procurement, management, and maintenance of software and systems for the university.

5. This CoP applies to all aspects of software development, procurement, management, and maintenance conducted by, or on behalf of, Leeds Beckett University.

6. It encompasses all Software and Systems, Development Environments, and Source Code and Repositories used in the development and management of software.

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. Software Development - The process of designing, coding, testing, and maintaining software applications and systems.

20. Software Procurement - The process of acquiring software from external vendors or third-party providers, including evaluation, selection, and purchase.

21. Software Management - The practices and processes involved in managing software throughout its lifecycle, including inventory management, version control, patch management, and secure installation.

22. Secure Coding Standards - Guidelines and best practices for writing software code that is secure and free from vulnerabilities.

23. Code Review - The process of systematically examining source code to identify and fix security vulnerabilities, bugs, and other issues.

RESPONSIBILITIES

Responsibilities and application of the CoP

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

25. 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.

26. Development Teams must adhere to secure development practices and participate in training and awareness programs.

27. Procurement Teams must ensure that all software procurement processes include security evaluations and compliance checks.

28. Digital Services Management must implement and maintain robust software management practices.

29. Head of Business Architecture must oversee the implementation of secure development practices and ensure compliance with relevant standards.

30. Department Head must ensure that their teams follow secure development, procurement, and software management practices and support ongoing training and awareness efforts.

31. All Staff and Students must report any security concerns or incidents related to software and systems.

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

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

OPERATIONAL APPLICATION

Software Management

33. All software procurement or installation should only be undertaken with the approval of Digital Services.

34. Robust software management practices, including inventory management, version control, and patch management, must be established to ensure all software is up-to-date and secure.

35. Security evaluations and compliance checks must be included in all software procurement processes to verify that software meets the university's security standards and regulatory requirements.

36. Secure installation procedures must be established to ensure that software is installed correctly and securely, minimizing the risk of introducing vulnerabilities.

37. The use of illegal software and using software for illegal activities is not permitted and may lead to disciplinary action.

38. All software installed on University computer systems must have an appropriate licenced by the university covering its intended use.

39. Use of software which tests or attempts to break university system or network security is prohibited unless the Digital Services Directorate has been notified and has given authorisation.

40. Use of software which causes operational problems, causes inconvenience to others, or which makes demands on resources that are excessive or cannot be justified, will be prohibited.

41. Software found on University IT systems and services that incorporates malware of any type is liable to be automatically or manually removed or deactivated.

42. For all University owned and managed equipment, formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software.

43. All changes to operating systems and ancillary software must be properly authorised and must be tested appropriately before changes are moved to the live environment to ensure there is no adverse impact on University operations or security.

44. All development, procurement, and software management activities must comply with relevant standards and regulations.

45. Secure development, procurement, and software management practices should be regularly reviewed and improved based on feedback, audits, and emerging threats.

46. There must be a nominated individual or business unit responsible for every item of software deployed on the University network.

47. Software applications are to be managed by suitably trained and qualified staff to oversee their day to day running, and to preserve security and integrity in collaboration with nominated individual application owners.

48. All staff managing software applications shall be given relevant training in information security issues.

49. The procurement or implementation of new or upgraded software (whether onsite or hosted in the cloud) must be carefully planned and managed in conjunction with Digital Services. Any development for or by the university must document the requirements for Information Security.

50. Information security risks associated with the procurement or implementation of new, or upgraded, software must be mitigated using a combination of procedural and technical controls.

51. All software implemented should be subject to the University's release management, version control, and change approval and management processes.

Software Development

52. Modifications to vendor supplied software shall be avoided as far as possible, and only strictly controlled essential changes shall be permitted, after agreement with the vendor and Digital Services.

53. The development of interfacing software shall only be undertaken in a planned and controlled manner.

54. Upgrades or other changes to locally developed software must be assessed to mitigate any potential risk to information security.

55. Secure coding standards must be enforced to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.

56. Regular training and awareness programs must be offered on secure development, procurement, and software management practices for all developers, procurement teams, and relevant stakeholders.

57. Rigorous code review and testing processes must be implemented to identify and remediate security vulnerabilities.

58. Development and testing environments, source code, and software management systems must be configured securely in line with other applicable university policies and procedures, with access restricted to authorized personnel only.

59. The security of third-party components and libraries used in development, procurement, and software management must be assessed and managed.

60. A structured change management process must be followed to ensure that all changes to software and systems are reviewed, tested, and approved before deployment.

61. Procedures for responding to security incidents related to software and systems, including timely reporting and remediation must be followed.

62. The use of live data in development and testing environments should be avoided.

COP MANAGEMENT

CoP Review

63. 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.

64. 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.

65. 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.