Patch Management Code of Practice

Executive Summary

This document describes the requirements for maintaining up-to-date systems, software and services across the Leeds Beckett University IT Environment.

The University has a responsibility to uphold the confidentiality, integrity and availability of data, and an obligation to provide appropriate and adequate protection of all its IT environment whether physical, virtual, on premise or in the Cloud.

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. As part of this commitment, we have established a comprehensive Patch Management CoP to ensure that all software and hardware components are regularly updated with the latest patches.

2. This CoP is designed to protect our information systems from the exploitation of vulnerabilities by threat actors, and to support the university's mission of providing a secure and reliable educational environment.

3. By adhering to this CoP, we aim to safeguard our digital assets, maintain stakeholder trust, and promote a culture of continuous improvement in our information security practices by regularly reviewing and updating patch management practices.

Purpose

4. The purpose of this Patch Management CoP is to establish a structured and consistent approach to managing software patches across the University IT Environment.

5. This CoP aims to ensure that all software and hardware components are up-to-date with the latest security updates and patches to protect against vulnerability exploitation and potential cyber threats such as malware.

6. It aims to ensure that patches are implemented in a manner that minimises disruption to university operations through risk assessment, ensuring that critical academic and administrative functions continue smoothly.

7. It aims to define clear roles and responsibilities for the identification, evaluation, prioritisation, testing, deployment, and verification of patches, ensuring accountability at all levels.

8. 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

9. This CoP applies to all assets, systems and services that comprise the University IT Environment.

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

11. 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.

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

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

Standards

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

15. 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

16. 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.

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

18. Assets – 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)

19. 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

20. 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.

21. 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.

22. 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.

23. Malware - a piece of 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.

24. 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.

RESPONSIBILITIES

Responsibilities and application of the CoP

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

26. 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)

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

OPERATIONAL APPLICATION

Software updates and patching

28. The University IT Environment must run up-to-date and patched Operating Systems and software. Where this is not possible compensating controls must be agreed and signed off by the Digital Services Leadership Team.

29. New systems must be patched to a current, agreed baseline before going live to limit the introduction of vulnerabilities.

30. Systems that are removed from the network because of insufficient patching will only be reconnected when it can be demonstrated that they have been brought up to date and no longer present a risk to the University IT Environment.

31. Third party suppliers must be prepared to provide evidence of up-to-date patching before IT systems are accepted into operational service.

32. Patching activity should be conducted in accordance with the following principles;

Identification

33. Regular monitoring of intelligence sources, such as vendor websites, security bulletins, and threat intelligence feeds, must be conducted so that new updates and patches are identified.

34. Applicable patching cycles or windows should be documented and patching activity conducted in line with these.

35. Activity designed to proactively identify vulnerabilities in the University IT Environment must also be conducted regularly, such as penetration tests, vulnerability scans, and SOC/SIEM monitoring, with results distributed and actioned in line with this CoP.

36. An inventory of all software and hardware to ensure all components should be maintained so that patchable assets are covered.

Evaluation

37. The criticality of new updates and patches must be assessed based on the potential impact to the University IT Environment.

38. Update and patches should be prioritised according to their severity and the risk they mitigate.

Testing

39. Update and patches should be tested in a controlled environment using appropriate test systems or pilot groups that closely matches the production systems to ensure they do not adversely affect system functionality.

40. Where there is no Test system then patch results from another non-key production system will be used and the results of any patch will be closely monitored for adverse effects.

41. The results of testing and any issues encountered should be documented.

42. User Acceptance Testing (UAT) of business systems should be considered after significant patching activity.

Deployment

43. To protect the University's IT systems from vulnerability exploitation, security updates and patches must be deployed in a suitable time frame based on a risk assessment considering the criticality of the patch i.e. 'Critical, 'High' etc.

44. Updates and patches should be applied in a manner that minimises disruption to university operations.

45. The application of software updates and patches should be automated where appropriate.

46. Where update or patch deployment is not possible, either appropriate compensating controls or a temporary means of mitigation must be applied to reduce the exposure faced by the University's IT systems.

47. Exceptions to the patch management CoP require formal documented approval from the Digital Services Leadership Team.

Verification

48. The successful application of patches should be verified post-deployment.

49. A remediation plan that allows for the return to a working state must be in place prior to any patching in the event of an unsuccessful patch deployment. This could be either rolling back to a last known good state or fixing forward.

50. Users with patching roles are required to compile and maintain reporting metrics that summarise the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

COP MANAGEMENT

CoP Review

51. 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.

52. 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.

53. 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.