v1-29Apr26

Logging and Monitoring Policy

1. Purpose

The purpose of this Policy is to ensure that Bath Spa University implements effective, proportionate and lawful logging and monitoring controls to:

- Protect the confidentiality, integrity and availability of university systems and data
- Detect, investigate and respond to security incidents
- Support compliance with legal, regulatory and contractual obligations
- Provide assurance to stakeholders and governing bodies

2. Scope

This Policy applies to:

- All University IT systems, networks and cloud services
- All users including staff, students, contractors and third parties
- All devices accessing University systems (managed or BYOD where permitted)
- All data classifications, including “Red data”

This includes monitoring of:

- User activity
- System and network events
- Security controls (e.g. authentication, endpoint protection)
- Third-party hosted services

3. Principles

Lawful and Transparent Monitoring

3.1 Monitoring will be conducted in accordance with:

- UK GDPR and Data Protection Act 2018
- Investigatory Powers Act (where applicable)
- Human Rights Act

Monitoring will be:

- Proportionate
- Risk-based
- Clearly communicated to users

Security and Risk-Based Approach

3.2 Logging and monitoring controls will be implemented based on:

- Risk to university systems and data
- Data classification (aligned to Information Classification Scheme)
- System criticality

Higher levels of monitoring will apply to:

- Systems processing personal or “Red data”
- Privileged accounts
- Internet-facing systems
- Identity and access system

Centralised and Correlated Monitoring

3.3 The University will implement centralised logging and monitoring capabilities where feasible to:

- Aggregate logs across systems
- Detect anomalous or suspicious behaviour
- Support incident response

Accountability and Governance

3.4 Monitoring activities will be governed through:

- Infrastructure Governance, Procurement and Compliance Group
- IT Services security function
- Data Protection Officer (for privacy oversight)

4. Logging Requirements

Minimum Logging Standards

4.1 All systems must generate logs sufficient to:

- Identify users and actions
- Record authentication events (success/failure)
- Capture administrative activity
- Record system changes
- Detect security events

Time Synchronization

4.2 All systems must:

- Use a consistent time source
- Ensure timestamps are accurate for forensic investigation

Log Integrity and Protection

4.3 Logs must be:

- Protected from unauthorised access or alteration
- Retained securely
- Stored separately from production systems where possible

Retention

4.4 Log retention periods must:

- Meet legal and regulatory requirements
- Support incident investigation

Typical baseline:

- Security logs: minimum 90 days searchable, 12 months retained
- Critical systems: extended retention where required

5. Monitoring and Detection

Continuous Monitoring

5.1 The University will implement monitoring capabilities to:

- Detect suspicious or anomalous behaviour
- Identify potential security incidents
- Alert appropriate teams
- Malware or endpoint compromise
- Data exfiltration attempts
- Policy Violations

6. User Activity Monitoring

Acceptable Monitoring

6.1 The University may monitor:

- System access and usage
- Network activity
- Email and collaboration tools (metadata and, where justified, content)

Monitoring will not be intrusive beyond what is necessary.

Privacy Safeguards

- Monitoring must be proportionate and justified
- Access to monitoring data must be restricted
- Investigations involving individuals must involve HR and/or DPO where appropriate

7. Third Party and Cloud Services

7.1 All third-party systems must:

- Provide adequate logging capability
- Allow integration with university monitoring systems where possible
- Meet contractual security requirements

8. Incident Response Integration

8.1 Logging and monitoring must support:

- Incident detection
- Investigation and forensic analysis
- Evidence gathering

Logs must be available to support:

- Internal investigations
- Regulatory reporting

9. Roles and Responsibilities

9.1 Chief Information Security Officer (CISO)

- Defines monitoring strategy
- Ensures alignment with regulatory frameworks

9.2 IT Services

- Implements logging and monitoring controls
- Responds to alerts

9.3 Data Protection Officer (DPO)

- Provides oversight on privacy implications
- Ensures compliance with UK GDPR

9.4 System Owners

- Ensure appropriate logging is enabled

- Support monitoring and incident response

9.5 All Users

- Must comply with acceptable use and security policies
- Must not attempt to bypass monitoring controls

10. Compliance and Enforcement

10.1 Failure to comply may result in:

- Disciplinary action
- Removal of access
- Legal or regulatory action

11. Exceptions

11.1 Any exception must be approved by:

- CISO
- Data Protection Officer (where privacy implications exist)

12. Continuous Improvement

12.1 The University will:

- Regularly review monitoring effectiveness
- Align with evolving threats and sector guidance

Document Details

Responsible Office: IT Services

Responsible Officer: Chief Information Officer

Approving Authority: Vice-Chancellor

Date of Latest Approval: 28 April 2026

Effective Date: 29 April 2026

Related Policies and Procedures: Information Security Policy, Data Protection Policy, Computer Use Regulations

Supersedes: (New)

Next Review Due: April 2029