Information security University of Bristol

System Management Policy (ISP-11)

1. Introduction

This System Management Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the responsibilities and required behaviour of those who manage computer systems on behalf of the University.

2. Scope

The University's computer systems will be managed by system administrators to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability). These system administrators will undertake their duties in collaboration with Technical Service Managers and subject matter experts whose services are running on these computer systems. This policy applies to all members of staff who use administrator (or elevated) privileges on any University multi-user computer system (server) to administer the system or the services running on the system. The management of desktop systems and autonomous networks is not in scope. For further information on the use and operation of Autonomous Networks see the guidance on Autonomous Networks (sharepoint.com).

3. Policy

3.1. Duties and Responsibilities

System administrators and Technical Service Managers are in uniquely privileged positions and play a key role in ensuring the security of the University's systems and services. They are expected to be aware of the University's Information Security policy in its entirety and must always abide by the policy.

System administrators and Technical Service Managers are responsible for ensuring the on-going security of their systems and must apply security patches in a timely manner or with other compensatory control measures taken to mitigate risk, in line with the IT Services Patching Policy. They are also responsible for ensuring system hardening (see 3.3 Security Hardening) baselines are maintained and that security event logging and monitoring services are operational at all times.

System administrators and Technical Service Managers are authorised to act promptly (within guidelines specified by change management) to protect the security of their systems but must be proportionate in the actions that they take, particularly when undertaking actions that have a direct impact on the users of their systems. Any actions that may be potentially invasive of users' reasonable expectations of privacy must be undertaken in accordance with the University's Investigation of Computer Use Policy (ISP- 18) and the associated Guidelines for system and network administrators document (PDF).

System administrators and Technical Service Managers are responsible for the raising of cyber operational risk where systems are unable to comply with this policy.

System administrators and Technical Service Managers must immediately report any information security incidents to the Information Security Team by emailing cert@bristol.ac.uk.

For the purpose of compliance to standards and policies, IT Services must maintain administrative access to all University computer systems, including those where system administrators and Technical Service Managers are not members of IT Services.

3.2. Access Control

Access to all computer systems must be via a secure authentication process, with the exception of read-only access to publicly available information. Wherever possible, authentication should be either via the University's single sign on service or against the University's central authentication database. Locally administered accounts should be avoided wherever possible.

Access and level of account privilege must be granted and managed in accordance with the User Management Policy (ISP-08).

Administrator accounts and accounts with elevated privileges must only be used when necessary, in order to undertake specific tasks which require the use of these accounts. At all other times, the principle of "least privilege" should be followed.

Use of administrator accounts (whether direct or indirect) should be conducted from University owned and managed devices via a trusted network only, unless a specific exception for risk is granted by Information Security Manager.

Multi-factor authentication should be used wherever available.

3.3. Security Hardening

Systems should be built and deployed to agreed secure baselines (i.e., systems will be hardened - this may include hardware, network, application and OS hardening methods).

Baselines will be agreed with the University IT Architecture Board (ITAB) and will be defined for hypervisors (where relevant), operating systems, applications and any required "middleware". Baselines must be reviewed by ITAB annually.

3.4. Security Event Logging and Monitoring

To support the visibility of systems to the teams responsible for the security of the University, all computer systems must have endpoint detection and secure operational logging enabled to standards agreed by ITAB.

Where operational constraints conflict with this requirement, any exception to this policy must have the risk and alternative mitigations documented and approved by the IT Services Senior Leadership Team.

The use and attempted use of all computer systems should be logged. The data logged should be sufficient to support the security, compliance and capacity planning requirements of the system but should not be unnecessarily intrusive. Users of systems should be given clear information of what information is recorded, the purposes of the recordings and the retention schedule of the data collected.

The UK data protection legislation requires that any personal data collected is collected for specific purposes and that it should be deleted when it is no longer needed.
It is recommended that log files are recorded on a different system from the system being monitored.

Audit logs should be configured to record any actions undertaken using administrator or elevated privileges. Audit logs should be secured to protect them from unauthorised modification.

3.5. Vulnerability Scanning and Penetration Testing

All systems should be subject to regular vulnerability scans and after any significant change has been made to a system – based on standards agreed by the IT Architecture Review Board). These scans may be undertaken by appropriately skilled and authorised University staff, or by approved and authorised external assessors. Business critical systems and other systems used to process or store data classified as confidential or above should be subject to regular penetration testing by an approved external assessor.

3.6. System Clocks

All system clocks must be synchronised to reliable time sources. These sources will be the University's official internal time servers, with the exception of these official internal servers themselves which will be configured as per internal IT Services service designs.

4. Further Guidance

- Guidelines for system and network administrators (PDF)
- User Management policy ISP-08
- Investigation of Computer Use policy ISP-18
- IT Architecture Board (ITAB) Terms of Reference

Title	System Management
Reference	ISP-11
Status	Approved
Version	3.0
Date Created	March 2014
Last Reviewed	May 2024
Next Review	May 2025

Classification	Public
PDF Policy Link	ISP-11 System Management Policy (PDF, 185kB)