University of Bristol
Information Security Policy

Title:	**System Management**
Reference:	**ISP-11**
Status:	**Approved**
Version:	**1.2**
Date:	**March 2014**
Reviewed:	**February 2019**
Classification:	**Public**

Contents

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.

Scope

The University's computer systems will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability). These system managers will undertake their duties in collaboration with individual technical service managers 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 is not in scope.

Duties and responsibilities

System and 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 managers should assign a business criticality level to their systems and ensure that their systems are registered in IT Services' asset database (Configuration Management Database). Depending on the level of criticality, they are responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service.

They should also assign (and record) a confidentiality level to their systems which indicates the suitability, or otherwise, of using any individual system for the storage or processing of different categories of University data (see the Information Handling Policy – ISP-07). This is in order to allow data owners to make informed decisions as to whether the system meets their security requirements.

Technical service managers are responsible for ensuring that their services are registered in IT Services' Service Catalogue.

System managers should deploy systems to agreed secure baselines (systems will be "hardened"). Baselines will be agreed with University IT Security specialists and will be defined for hypervisors (where relevant), operating systems, applications and any required "middleware". Baselines must be reviewed from time to time.

System managers are also responsible for ensuring the on-going security of their systems and must apply software patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches must be applied in accordance with software suppliers' recommendations (or requirements) or within 5 working days of release, whichever is the shorter. If it is not possible to patch within this time period, other compensatory control measures must be taken to mitigate risk.

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

System managers must immediately report any information security incidents to the Information Security Manager (or, if unavailable, by email to cert@bristol.ac.uk).

Change management

All changes to computer systems are subject to IT Services' established change management processes and procedures.

File integrity monitoring software should be used to help detect unauthorised system changes.

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 must only be granted in strict 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.

Access to administrator accounts (whether direct or indirect) from untrusted networks (from home, for example) or when using personally owned devices should be protected by two-factor authentication wherever possible.

Monitoring and logging

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. This information should be made available to users in the form of a system specific privacy policy.

The Data Protection Act 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.

Vulnerability scanning

All systems should be subject to regular vulnerability scans (at least every 12 months and after any significant change has been made to a system). These scans may be undertaken by appropriately skilled University staff or by approved external assessors. Business critical systems and other systems which are used to process or store data classified as strictly confidential or above should be subject to regular (at least annual) penetration testing by an approved external assessor.

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 must be synchronised with official JANET time servers.

Further guidance

The "Guidelines for system and network administrators" document is available at:

http://www.bristol.ac.uk/infosec/policies/docs/sysadmin.pdf

The Configuration Management wiki which includes links to information about the Configuration Management Database, the Data Dictionary and the Service Catalogue is available at:

https://wikis.bris.ac.uk/display/ITIL/Configuration+Management