Policy: **ISP-S11**
Title: **System Management Policy**
Status: **Approved**

1. Introduction

1.1. This information security policy document sets out responsibilities and requirements for those managing computer systems. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- System manager - someone who configures and maintains a multi-user computer or software application service.
- Back out plan - a planned course of action to restore a system to its previous state should a change fail to successfully complete or causes an undesirable effect.

1.3. This document includes statements on:

- System managers
- Responsibilities and duties of system managers
- System change management
- Access control
- Monitoring and logging system activity
- Importing software and files
- System clocks

2. System managers

2.1. University computer systems must be managed by competent staff to oversee their day-to-day running and to preserve security and integrity:

2.2. System management policy applies to all staff that use administrator privileges on any University multi-user computer or software application service.

3. Responsibilities and duties of system managers

3.1. System managers have a key role to play in ensuring confidentiality, integrity and availability of University information and information systems. They are responsible for endeavouring to ensure correct and secure operation of computers in accordance with both University level policies and any relevant departmental policies.

3.2. Computer system managers are required to be aware of University information security policies in general. They must be familiar with this document and these other documents which are of particular relevance to system managers:

- Network Management Policy (ISP-S12)
- Information Handling Policy (ISP-S7)
- Software Management Policy (ISP-S13)

- Use of Computers Policy (ISP-S9)
- Computer Account Passwords (ISP-I9)
- Institutional IT Usage Monitoring and Access (ISP-I6)

3.3. System managers must take into account the confidentiality and value of the information they are managing, and the impact that a serious incident may have, when determining what security controls and risk mitigation measures to use. It is recommended that system managers perform a risk assessment on deploying new systems and from time to time thereafter. See also:

- Managing Information Asset Security (ISP-I4)

3.4. System managers are required to be proactive in working with information owners to help ensure that security requirements, expectations and limitations are mutually understood and agreed. A basic example of this is to ensure that information owners are aware of the backup arrangements, ensure that backups take place as specified and keep information owners informed of any changes or problems. For policy on making backups refer to the “Backups” section of:

- Information Handling Policy (ISP-S7)

3.5. Basic information about the security posture of a computer system should be made available to its users by the system manager. This is intended to enable information owners or custodians to make an informed decision as to whether the system meets their security requirements. This information should not include any details that would be of practical use to potential intruders; however, it might outline:

- Physical security of the system and its data storage.
- Access control.
- Operating environment.
- Backup frequency and security of backup data.
- Firewalling and protection against malware.
- Monitoring and systems administration staffing.
- Relevant policies implemented.
- Uses for which the system is not suitable.

3.6. Recognised managers of computer and network systems are encouraged to promote and implement information security policy. They are authorised to act promptly to protect the security of the systems and information for which they have responsibility. There must, however, be reasonable grounds for taking actions which impact users such as: temporarily removing devices from the network, disabling software or system functionality, or locking user accounts.

3.7. System managers and staff who have elevated access privileges are prohibited from going beyond the boundaries of their legitimate professional duties in relation to accessing users’ computer data. Any access to, or disclosure of, the contents of user data or communications must be appropriate, justified and follow correct procedures. See:

- Institutional IT Usage Monitoring and Access (ISP-I6)

3.8. System managers must be vigilant and immediately seek advice through their line management if they become, or are made, aware that any information served by the systems for which they have responsibility may:

- Not be lawful.
- Contain direct links to material which is unlawful.
- Purport to trade on the University's name in a commercial activity or goods without the approval of the University.
- Promote unapproved commercial activity.
- In any way damage the University's name or reputation.
- Not comply in some other way with University policies.

4. System change management

4.1. Changes to computer systems that provide a user service must be planned, tested, approved, publicised and implemented in a controlled manner.

- It is recommended that an appropriate “change management” procedure is established and followed for systems other than those managed and used exclusively by an individual user and where the changes would not put at risk other University systems or services.
- The change management procedure should involve stakeholders, create an audit trail, consider security implications, and include communication to users about forthcoming changes. (Change management is intended to help minimise and manage undesirable impacts on service users and the business.)
- The planning and testing of changes should include consideration of security factors including: information confidentiality requirements, data access controls, exposure of network services, known issues with software, data backup and the business continuity plan.
- Preparation for a change should include formulation, and where possible testing, a “back out plan”.
- Where possible, and always for key systems, testing should be undertaken in a separate test environment or using another method that avoids significant risk to the service.
- Changes to systems must be approved by management before made live or moved to the live environment.
- System managers should ensure that system users are advised about forthcoming changes before implementation.

4.2. IT Services staff manage changes to central services using a procedure based on Information Technology Infrastructure Library (ITIL). Some staff in other departments are able to implement changes either directly to IT Services managed systems, or changes which may significantly affect operation of those systems. Those departmental staff must submit proposals for such changes to the IT Services change management system for approval before implementation.

5. Access control

5.1. Access to all University information services and computer systems must be via a secure log on process, except for read-only access to public domain information.

5.2. Granting of access to University IT resources should be carefully controlled. There should be formal procedures in place for granting, changing and revoking access to information systems and services for handling the various scenarios. See:

- User Management Policy (ISP-S8)

5.3. University IT system managers must wherever technically possible enforce password policy. See:

- Use of Computers Policy (ISP-S9)
- Computer Account Passwords (ISP-I9)

5.4. The individual responsible for each computer account must be identifiable. This also applies to group accounts to the extent that the individual responsible for management of the account is known and can identify all others with access. See also:

- Use of Computers Policy (ISP-S9)

5.5. The Administrator account, or administrator level access, should be used only at times when it is necessary to perform specific system administration or configuration tasks. (Unnecessary routine use of administrator level access by system managers has been a factor in many system compromises.)

5.6. System managers must ensure that user privileges are configured on the basis of "least privilege", i.e. users should not be granted privileges to do things that they do not need to do and which might cause problems. Access to any operating system commands and utility programs which elevate the privilege of the user should also be appropriately restricted.

5.7. System managers should normally not allow users to work with elevated privileges (for example by placing normal user accounts in the "Administrator" or "Power Users" group on Windows systems). In exceptional cases, for example where technical problems require elevated privileges to make legacy or badly designed applications work, system managers should endeavour to work round or remove the problems - there is usually a more secure solution.

5.8. Access to files, folders and other resources should, wherever possible, be managed using group permissions rather than by individual account. The purpose, or intended membership, of each group should be defined clearly, for example "users", "administrators", "backup operators", "managers" etc. The membership of each group should be correctly set and periodically reviewed.

5.9. Wherever appropriate and possible, systems and applications should be configured so that inactive connections shut down after a defined period of inactivity to help prevent access by unauthorised persons.

5.10. Recommended access controls for sensitive or high risk systems include:

- Allocate privileges through a formal authorisation process.
- Maintain a record of any access permissions granted that exceed basic user permissions.
- Maintain documentation of the purpose or intended membership of user groups.
- Log and preferably actively monitor access to help identify signs of misuse.

5.11. For very sensitive or high risk systems additional recommended access controls include:

- Limit privileged access according to physical or network location.
- Control privileged access based on time of day.
- Use of secondary security tokens.
- Use a secure console server arrangement.

6. Monitoring and logging system activity

6.1. Logging and monitoring of computer system activity should be implemented to adequately support security, compliance and capacity management.

6.2. System managers must act on any current legal compliance requirements pertaining to logging that apply to their systems.

6.3. The Data Protection Act requires that personal data is deleted when no longer needed for the purpose for which it was originally obtained. Procedures should therefore be implemented to ensure obsolete log data containing personal data (such as usage information by username) is deleted.

6.4. For systems where an intrusion or misuse could have a significant impact on the University, at the minimum, basic usage logging should be undertaken. This may consist of recording logs showing when users were logged in, when they accessed system resources etc.

6.5. Where logging is undertaken with a view to possibly using the logs as evidence in the case of an intrusion, then it is recommended that the logs are recorded on a different system to the one being monitored. (Usage logs are likely to be deleted or modified by an intruder.)

6.6. System logging can often be configured to record both successful and failed attempts to access system resources. For sensitive systems, audit logging may be configured to record access failures, which may indicate an intrusion attempt or operational problem.

6.7. Capacity demands of systems supporting business processes should be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available. System managers should report capacity risks or concerns that they have identified to their line manager.

6.8. Major systems, configured to produce useful levels of security and operational log information, typically produce more data than it is realistic to monitor manually. Where the sensitivity of a system justifies it, use of automated log monitoring and alerting technology is recommended to help make best use of security and operational log data.

7. Importing software and files

7.1. Software and data files intended for installation on critical computer systems should be downloaded or installed into a secure environment, scanned for malicious software and tested in a test environment before deployment in a live environment.

8. System clocks

8.1. All networked computers should be referenced to a reliable time server. Incident investigation often depends on accurate event log dates and on examining creation and modification dates of files and folders.

Failure to comply with University Policy may lead to disciplinary action.

Document history:

06	October	2009	(C. Nelson)	Began first draft.
06	July	2010	(C. Nelson)	Steering Group changes: • Changed scope of this document such that it does not apply to those who only administer their personal computers (as distinct from multi-user services). • In 2.1 replaced “should” with “must” and “suitably trained and qualified” with “competent”. • In 2.1 removed bullets: “Wherever possible system management tasks should be undertaken by professional departmental or central computing staff” and “All systems management staff should be given general training on information security relevant to their role and sufficient specialised training to securely operate the systems they are required to manage.”
16	August	2010	(C. Nelson)	ISP-I4 is renamed “Managing Information Asset Security”.
14	October	2010	(C. Nelson)	“System managers must at all times take every reasonable care to ensure that all material which is served by systems for which they have responsibility...” was changed to “System managers must handle any reports or complaints about information, served by the systems for which they have responsibility, to help ensure that it...”.
02	November	2010	(C. Nelson)	Further revision of the section concerning System Managers’ responsibility relating to information being served, as recommended by the Steering Group.
18	May	2011	(C. Nelson)	Revisions resulting from review within IT Services.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.