GISP24. Systems management and development

Date:	5 October 2017
Version:	3.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
2.0	1/2/13	Inactivity timeout addition approved by ISSC
2.1	5/10/17	Reviewed and updated
3.0	20/10/17	Approved by ISSC

Policy

Security Control	Control of the installation, configuration, maintenance, development and management of information systems and the software and services they run.
Objective	To ensure that information security good practice is applied to the installation, configuration, maintenance, development and management of information systems.
Policy	24.1. The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security. 24.2. All systems must be regularly checked to ensure that they comply with the organisational security policy. 24.3. The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained. 24.4. Procedures will be established for the reporting of software malfunctions and faults in the organisation's information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken. 24.5. Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures. 24.6. Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

	24.7. Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the organisation must follow a formalised development process. 24.8. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals. 24.9. New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Assistant CIS Director. The business requirements of all authorised systems must specify requirements for security controls. 24.10. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Classification and Data Management policy, and a risk assessment undertaken to identify the probability and impact of security failure. 24.11. Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the organisation's information security policies, access control standards and requirements for on-going information security management. 24.12. Systems must be configured to industry-accepted security hardening standards. Before installation on the network, all vendor supplied defaults must be changed, and all unnecessary default accounts must be removed or disabled. 24.13. Systems handling payment card details (in the cardholder data environment), handling personal data, or forming part of the institution's key infrastructure must be subject to regular penetration testing by suitably qualified personnel following an agreed methodology. Penetration testing should be conducted at least annually, or after any significant infrastructure or application upgrade. 24.14. The organisation's systems are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual system owners. All systems management staff shall be given relevant training in information security issues. 24.15. Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff. Logs must record all actions by users with root or administrative privileges, invalid logical access attempts, and use of or and changes to authentication mechanisms. Logs must be written to a secure, internal log server. Any anomalies or suspicious behaviour identified must be followed up. 24.16. The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the organisation must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

	24.17. Inactive connections to the organisation's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.
Responsibility	• Data and system owners are responsible for ensuring their data and system is managed in accordance with the University's information security policies. • ITCS is responsible for ensuring all staff managing information services are managed by suitably trained and qualified staff.
Incident Management	Incidents should be reported to the IT Service Desk in the first instance who will escalate the incident as appropriate.
Implementation	Further information about information systems managed by ITCS is available from the ITCS web site at https://portal.uea.ac.uk/itservices/corporate-systems. See also GISP9 Change management. **Inactivity timeout period** When the system is implemented, ITCS will seek agreement with the system owner on an appropriate period of inactivity before automatic logout. The following points should be considered when deciding this period: • Whether auto logout of the system is supported by the system • Whether different periods are supported by the system for different user circumstances. If not, then the minimum required period will be applied to all users • The period should account for the risk of unauthorised access associated with the location of the computers accessing the system (e.g. whether they are located in publically accessible spaces) and the information classification of the information held on the system • The period should account for its impact on day to day activities.