GISP10. Protection against malicious software

Date:	5 October 2017
Version:	2.0
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
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	All computer systems must be protected against malicious software.
Objective	To prevent infection of all University computer systems by malicious software such as viruses, trojans, worms, key loggers etc.
Policy	10.1. All devices connected to the University network must have up to date security patches installed, and be configured to update automatically using ITCS provided central mechanisms wherever possible. 10.2. All devices connected to the University network must have University approved software installed that will protect against malicious software such as viruses, Trojans, worms, key loggers etc. where feasible. The software and associated data files should be installed and configured following defined policies and procedures. 10.3. All systems connected to the University internal managed network will be regularly scanned for vulnerabilities. All high risk vulnerabilities discovered must be resolved within 30 days (e.g. by installation of a security patch).
Responsibility	• ITCS will monitor malicious software threats and will provide central services for automatic updating of supported operating systems and approved software used to protect against such. • IT support staff are responsible for ensuring deployed systems have up to date operating system patches and anti-malware software installed and correctly configured. • All users have a responsibility for protecting against malicious software and particular care and vigilance should be taken when downloading files from untrusted sources.

Incident Management	• Any computer system found to be infected with malicious software will be disconnected from the network until the software has been removed. • Any computer system discovered to be not up to date in respect of either operating system patches, or anti-malware software will be immediately referred to the IT support staff responsible for that system and these will in turn remedy the situation as soon as possible.
Audit and accountability	IT Support Managers should ensure that a security audit of systems in their charge is carried out on a regular basis (at least annually) and remedial action undertaken where necessary.
Implementation	**Operating systems** • Computers running multiple operating systems, either via dual boot mechanisms, emulation, or virtual machines, should ensure that each operating system has up to date patches, security packs, anti-malware software installed, all of which should be automatically updated wherever possible. **Application software suites** • All application software suites should have the latest patches and security packs installed and wherever possible ensure that auto-update mechanisms for these are in place. **Firewall** • All operating systems should have their firewall switched on and any exceptions to the default firewall rule set are only to be allowed by agreement with IT support. **Anti-virus and anti-malware** • Anti-virus and anti-malware software should be installed and kept up to date. Auto update mechanisms for virus definitions etc. should be enabled. **Securing desktop computers against unauthorised access** • The number of local and privileged user accounts on workstations must be kept to an absolute minimum. • No workstations should allow remote access to any non-University members without prior permission from ITCS. • Users should not normally access workstations using accounts that have elevated privileges, except in specific cases where required by IT support – see GISP5 ‘Desktop local administrator accounts’. • Where elevated privileges to a computer have been requested and approved for a user, these should be enabled by IT Support staff using Active Directory group policies wherever possible and assigning specific rights for a user on a specific machine. • When a user leaves UEA employment or changes their roles/responsibilities any access rights or local accounts assigned to that user should be removed or modified as appropriate.