SM10.1 Anti-malware and workstation specific controls

Summary of main revisions March 2011

General

- Footnote inserted to clarify scope of term ‘workstation’.
- ‘ITCS’ changed to ‘Information Services’ throughout – consistent with other recent policy revisions.

Objective

- Malware scope broadened slightly

Responsibility

- Removed specific references to PCs and Macs to allow for future changes in support policies. Footnote gives link to Desktop Computer Operating System Policy
- Broadened focus to all supported application software as patches/service packs for any software can be relevant to security.
- Responsibility for security changed to IT Support Managers to be consistent with new structure. Should also cover for CMP where there should at least be a person in charge of their IT support who would be regarded as IT Support Manager.

Incident management

- Helpdesk now first port of call for reporting compromised workstations, will ensure all incidents properly logged/tracked.

- Link text to ‘cleaning’ procedures for compromised machines (link to be inserted when procedures reviewed and agreed by ISDMT, draft in separate document). Should enable more consistent dealing with such and ensure compromised workstations are not prematurely re-connected to network. Gives policy and procedures for IT support staff to refer to when resistance met.

Audit and accountability

- IT Support Managers now responsible for ensuring regular security audit of work stations carried out.

Implementation

Operating Systems

- Removed specific references to methods used to implement patching and updating and changed to more generic ‘Information Services provided central mechanisms’

Application software suites

- ‘Office application software suites’ changed to ‘Application software suites’ as other software should also be kept up to date with patches to ensure good security.
- Removed specific references to different operating platforms as software should be kept up to date with patches irrespective of the operating system.

Firewall

- Removed specific references to different operating platforms as same should apply to all.

Anti-virus and anti-malware

- Removed specific references to different operating platforms, now more generic.

CIS corporate applications

- Removed specific reference to workstations running CIS having to be in Active Directory, as all systems should now be in the AD

Securing desktop computers against unauthorised access

- Based on security consultants recommendations inserted controls to ensure that local and privileged user accounts are kept to an absolute minimum, and restriction on computers allowing remote access to any non-University members without prior permission from ITCS.
- Removed control re. extended access rights on computers not in AD, as all should now be in the AD.

Report Control Information

Title:	Security Manual - SM10.1 Anti-malware and workstation specific controls
Date:	9 June 2011
Version:	v1.1 (to be approved by ISSC)
Reference:	ICT/SECMAN/SM10.1/v1.1/DRAFT
Authors:	Steve Mosley
Quality Assurance:	ISSC

Revision	Date	Revision Description
V1	17/7/07	As approved by ISSC July 2007
V1.1	18/4/11	Reviewed and approved by ISDMT 13/4/11 for submission to June 2011 ISSC. Revisions as part of Security Review project and based on recommendations following external consultants report.

SM10.1 Anti-malware and workstation specific controls

Security Control	Workstation[1] controls to guard against malware and unauthorised access
Objective	To ensure that workstations are protected against malware attacks from viruses, worms, trojans, spyware and other malicious and unwanted software. To ensure that workstations are protected against unauthorised access.
Responsibility	Information Services will advise on best practice regarding computer security and provide appropriate site licensed client software for supported operating systems[2] to guard against malware. Information Services will also provide services for the automated distribution and install of security patches and service packs for supported operating systems and application software[3] suites. It is the responsibility of IT Support Managers to ensure that systems they are responsible for are adequately secured against malware and unauthorised access in accordance with the security controls documented here.
Incident management	Where any computer system is discovered, or judged, to be inadequately protected against malware or unauthorised access, this should be reported immediately to the IT Helpdesk who will log and pass to the appropriate IT support team. If a workstation is discovered to be compromised, the passwords of users of that machine should be changed as soon as possible and procedures for re-imaging the machine and 'cleaning' of associated storage resources should be implemented as per SP2 'Procedures for dealing with malware infected desktop computers'

[1] The term 'Workstation' in this policy should be taken to mean computers attached to the University network, including desktop, laptop/notebook and net book computers.

[2] For desktop computer operating systems policy see 'Desktop Computer Operating Systems Policy' at http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputeroperatingsystemspolicy

[3] For desktop computer software policy see 'Desktop Computer Software Policy' at http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputersoftwarepolicy

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** SM10.1.1 All computer systems should have up to date operating system security patches and service packs installed and be configured to update automatically using Information Services provided central mechanisms wherever possible. SM10.1.2 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** SM10.1.3 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** SM10.1.4 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** SM10.1.5 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** SM10.1.6 The number of local and privileged user accounts on workstations must be kept to an absolute minimum. SM10.1.7 No workstations should allow remote access to any non-University members without prior permission from Information Services. SM10.1.8 Users should not normally access workstations using accounts that have elevated privileges, except in specific cases where required by IT support – see Security Manual SM5.3 System Administrator Passwords, 'Desktop local administrator accounts'. SM10.1.9 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. SM10.1.10 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.