APPENDIX A: MINIMUM SECURITY STANDARDS FOR DEVICES ATTACHED TO THE CAMPUS NETWORK

Each device attached to the campus network must meet the following minimum standards.

SOFTWARE PATCHES

It is easy to identify exceptional cases, in the form of devices that can't be or shouldn't be patched for any number of good reasons – trying to get the spirit but also allow for exceptional cases is an editorial challenge which this version may or may not meet]

(a) Each device must run only software for which security patches (in the software or underlying operating system) are made available in a timely fashion.
(b) Each device must have all currently available security patches installed and operating, unless those patches are known to create problems with the execution of the device or its key applications, or to create new security problems.
(c) Temporary exceptions may be made only in the case of a patch that compromises the usability and/or reliability of a device running an application critical to the University.

ANTI-VIRUS SOFTWARE

There are exceptions to be handled carefully

(a) Each device for which anti-virus software is routinely made available must have appropriate anti-virus software installed, running, and operating in a mode in which it is regularly and automatically updated."
(b) Appropriate anti-virus software" means the software made available as "the campus standard" through the campus-wide software licensing program, or an alternative that is widely accepted as equivalent. If there is a question as to whether a particular alternative is acceptable, the potential user must get clarification from the IT Office before the software is purchased and installed.

HOST-BASED FIREWALL SOFTWARE

There are exceptions to be handled carefully

(a) Each device must have "host-based firewall" software installed and running.
(b) The default configuration for all host firewall must have all ports/services turned "off", so that ports/services are turned "on" only if and when required by the specific function of that device.
(c) This requirement for each device is independent of whether or not the device is part of a workgroup that has a separate firewall installed for that group.

AUTHENTICATION

(a) Access to all devices and/or services provided by those devices must be protected by means of secure passwords or other secure authentication processes (e.g., SmartCards, biometrics).
(b) To the extent possible with current technology, all forms of authentication in which authentication information passes across the network must use mechanisms which encrypt that information in a secure manner.
(c) To the extent possible with current technology, encryption is required for all but "direct authorization", e.g., typing a password directly into a workstation, using a SmartCard scanned by a reader attached directly to the workstation. In particular this means that legacy, insecure versions of applications such as Telnet, FTP, SNMP, POP, IMAP, and other must not be used, and must instead be replaced by modern versions that use encryption.

PASSWORDS

(a) The term "secure passwords" used #4 means use in conformance with minimum password complexity standards [add appropriate reference].

(b) For legacy applications/devices, this requirement can be waived only temporarily while those responsible for these applications/devices update their system's password mechanism to meet minimum standards.
(c) For new applications/devices, this requirement is absolute, i.e., a new application/device that does not support secure authentication must not be made available/connected to the network.

UNAUTHENTICATED EMAIL RELAYS

(a) A campus device must not provide an active SMTP service that allows unauthenticated parties to relay email messages, i.e., no device will process an email message where neither the sender or recipient is a local user.
(b) Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Note that authenticating the sending machine (e.g. IP address and/or domain name) rather than the sending user does not meet this standard.

UNAUTHENTICATED PROXY SERVICES

(a) Devices must not provide proxy servers/services which allow use by unauthenticated users, without prior written approval by the CIO upon advice from the IT Security Committee.
(b) Any software which provides proxy server/service capability must be installed with the default configuration in which such capabilities are turned "off".
(c) While there are some valid uses for unauthenticated proxy services, and the ITSC will approve their use in appropriate circumstances, in many cases such services are provided by accident (i.e., reliance on vendor defaults), failure to understand the alternatives that are available, or failure to assess properly the balance between the risk to the overall network vs. convenience to the device administrator. Local convenience is clearly at best a secondary factor, and generally will not be sufficient to justify ITC approval.

PHYSICAL SECURITY OF NETWORK CONNECTIONS AND DEVICES

(a) Installation, maintenance, and modification of all campus network devices is the sole responsibility of IT staff [UMH-NS-1]. This includes cabling, wiring, attachment jacks, network electronics, wireless connection devices, and all support equipment housed in network closets/cabinets. Access to and/or modification of this equipment is restricted to authorized central staff. Authorized user access is restricted to attachment of devices to authorized attachment devices or via authorized wireless connection facilities.
(b) Each device attached to the network must have a clearly identified "owner/operator" who is responsible for its use and conformance with these standards [UMH-NS-3]. For "wired" connections, the device owner/operator is assumed to be the unit identified as responsible for the wired network access point. For "wireless" connections, the device owner/operator is assumed to be the person identified as part of wireless authentication.
(c) Physical security should be maintained for each device in a manner consistent with the designated use of the device. Considerations should include protection from unauthorized physical manipulation (up to but not limited to theft), and ensuring that devices are configured to "lock" after a suitable idle period where re-authentication is required to "unlock" the device.
(d) Units may not provide "live" network access points to which they allow connection of transient devices for which they do not have owner/operator responsibility. In particular, units should use authenticated wireless access to permit students and others to connect with portable devices, rather than simply providing "open" wired access points.
(e) Individual units/users may not attach devices that have the primary function of providing wireless access to the campus network, i.e., unauthorized wireless access units are not allowed.
(f) Individual units/users that attach devices which provide as a secondary function wireless connection from a second device to services on the first device (e.g. a portable computer which supports a wireless

link to a PDA) must ensure that the wireless capabilities and support device are configured and operated in a manner that does not permit unauthorized access.