Minimum Security Standards for Network Devices

These minimum standards are intended to ensure the security of all Devices connected to the Campus Network. Any Device to be connected to the Campus Network must satisfy the following minimum standards, as appropriate, or adopt a standard alternate security measure (see Attachment B).

1. Software patch updates

Devices to be connected to the Campus Network must run software for which critical security patches are made available in a timely fashion and must have all currently available security patches installed.

Exceptions may be made for patches that compromise the usability of critical applications.

2. Anti-malware software

Anti-malware software for any particular type of operating system must be running and up-to-date on every Device, including clients, file servers and mail servers. Products other than offered by the campus may be used if comparable.

Exceptions may be made for anti-malware software that could compromise the usability of critical applications.

3. Host-based firewall software

System Administrators are responsible for ensuring that computers with native host-based firewall software included in the operating system have the firewall activated and properly configured.

Exceptions may be made for firewall software that compromises the usability of critical applications.

4. Passwords

Campus electronic communications systems or services that require users to be identified must identify and authorize users using secure authentication processes (e.g., digital certificates, biometrics, Smart Cards, one-time passwords or encrypted password transactions). When reusable passwords are employed, they must meet the minimum password complexity standards below. In addition, shared-access systems must be configured to enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible Devices must be modified.

Passwords that may be used by System Administrators for their personal access to a service or Device must not be the same as those used for privileged access to any service or Device.

All passwords employed to authorize access to campus electronic communications systems or services must meet the following minimum password complexity standards. The password *must:*

- Contain eight characters or more.
- Contain characters from at least two of the following three character classes:
    - Letters (a-z, A-Z)
    - Numbers (0-9)
    - Special characters including a space (: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

5. Unencrypted authentication

Unencrypted Device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the Campus Network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. To prevent password harvesting, passwords must not be sent in the clear and all campus Devices must use encrypted authentication mechanisms or otherwise secure authentication mechanisms. Passwords or protocols which provide no log on access to the system (e.g., anonymous FTP) are exempted from this requirement.

6. Unauthenticated email relays

Campus Devices must not provide an active SMTP (an Internet protocol for sending email between Devices) service that allows unauthorized parties to relay email messages. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Unless an unauthenticated relay service has been reviewed by Information Technology Services as to configuration and appropriate use, it may not operate on the Campus Network.

7. Unauthenticated proxy services

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate Device configuration.

Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by Information Technology Services as to configuration and appropriate use, it is not allowed on the Campus Network.

In particular, software program default settings in which proxy servers are automatically enabled must be identified by the System Administrator and re-configured to prevent unauthenticated proxy services.

8. Physical security

Unauthorized physical access to an unattended Device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, Devices must be configured to “lock” and require a user to re-authenticate if left unattended for more than 20 minutes.

System Administrators are responsible for maintaining the physical security of devices in their care.

9. Unnecessary services

If a service is not necessary for the intended purpose or operation of the Device, that service shall not be running.