Policy Title	Original Adoption Date	Policy Number
Minimum Security Standards for Network Devices	01/19/2015	IN-711
Responsible College Division/Department	**Responsible College Manager Title**	
Information Technology Services	Director of Information Technology	

Policy Statement

I. PURPOSE & APPLICABILITY

The purpose of this policy is to establish the Minimum Security Standards for all electronic Devices connecting to the LTC Network. Such standards serve to help protect not only the individual Device, but other Devices connected to the LTC Network. This policy also identifies those with principal responsibility for compliance with the Minimum Security Standards, and for the enforcement of this policy, including taking corrective action.

This policy applies to all faculty, staff, students and contractors who connect a Network Device to the LTC Network. (i.e., when a Network Device will be assigned an Internet Protocol (IP) address that is routable on the LTC Network and, can be used to send data to, or receive data from, the LTC Network). This policy is applicable:

- regardless of how the Device is connected to the LTC Network (e.g., directly from a campus office or indirectly from a faculty/staff member's home, for example using LTC Virtual Private Network (VPN)); and
- whether or not the Device is owned by LTC.

Whenever anyone is connected to the LTC Network, he or she is expected to comply with this Policy.

II. STATEMENT

All Devices connecting to the LTC Network, whether physically located on campus property or not, must comply with the Minimum Security Standards outlined below. A Device that does not meet these Minimum Security Standards is subject to disconnection or having its access blocked to the LTC Network until remediation has been performed. More restrictive standards may be adopted at the department or unit level.

Devices that host sensitive or confidential data as defined in LTC's Policy on Protection of Electronically Stored Personal Information may be required to conform to more rigorous security standards.

Minimum Security Standards for Network Devices

These minimum standards are intended to ensure the security of all Devices connected to the LTC Network. Any Device to be connected to the LTC Network must satisfy the following minimum standards:

1. Software patch updates

Devices to be connected to the LTC 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-virus software
Anti-virus 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 college may be used if comparable. Exceptions may be made for anti-virus software that could compromise the usability of critical applications.

3. Host-based firewall software (software on a Device that helps protect the Device by controlling what network traffic is allowed to enter and leave the Device) 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
LTC 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. Further, these passwords are set to expire every 120 days, requiring a reset by the end user. Expiration dates will be set to coincide with semester starts, if possible.

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 both alphabetic and numeric characters; at least one alphabetic character must be uppercase (e.g.: A-Z), and at least one alphabetic character must be lowercase (e.g.: a-z).
- Not contain the user's first name, last name or username.

5. Unencrypted authentication
Unencrypted Device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the LTC 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 LTC 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
LTC 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 LTC 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 LTC 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 15 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.

Reason for Policy

LTC encourages the use of its electronic communications network in support of the College's mission. However, this resource is limited and may be vulnerable to attack or improper use. It must be well-managed and protected, and LTC reserves the right to deny access to its electronic communications network by Devices that do not meet its standards for security.

Historical Data, Cross References and Legal Review

Reviewed/Revised
Legal Counsel Review and Approval:
Board Policy:

Definitions

LTC Network: All LTC networks, wired or wireless, that are connected to the college's core network, directly or indirectly, and whether or not behind a firewall or Network Address Translation (NAT) device. (NAT is an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic).

Network Device (Device): Any computer, Smartphone, tablet, iPad, printer, wireless appliance or other piece of equipment that can connect to and communicate over the LTC Network.

System Administrator: An individual who installs, configures and/or maintains any Device in his or her

area of responsibility that is connected to the LTC Network.