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**	
Technology Division	Vice President of Administration	

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 employees, 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 an employee'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. 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. 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.

5. 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.

6. 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

Created: 2015
Reviewed/Revised: 10/22/20

Legal Counsel Review and Approval:
Board Policy: III.A. General Executive Constraint, III.B. People Treatment

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.