UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-3001	**Policy Title:**	Network Device Connectivity Policy
Effective:	11/18/2016	**Responsible Office:**	Information Services
Date Approved:	11/18/2016	**Approval:**	Vice President for Information Services & Chief Information Officer
Replaces Policy Dated:	N/A	**Responsible University Official:**	Vice President for Information Services & Chief Information Officer

SCOPE:

This policy applies to the University of Richmond and all of its Affiliates. As used in this policy, the term "Affiliates" means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board.

INDEX:

IRM-3001.1.....Definitions

IRM-3001.2.....Policy Statement

IRM-3001.3……Applicable Regulations and Accreditation Standards

POLICY STATEMENT:

IRM-3001.1 – Definitions

Workstations

Workstations are general use devices that run either the Microsoft Windows or Mac OS X operating system. They generally fall into one of the following sub-classes:

1. Primary and secondary workstations provided to faculty, staff, volunteers, and contractors by Information Services
2. Consumer desktops and laptops brought to campus by students
3. Workstations located in computer labs across campus and in Boatwright Library

Servers

A server is a device that provides shared resources such as file shares, printers, or an application to one or more users over the network. They are typically located in one of the campus data centers. They may run on dedicated physical hardware or may be virtualized running on a hypervisor.

1. Microsoft Windows Servers
2. Red Hat Linux Servers
3. Mac OS X Servers

Smart Devices

1. Cellular Telephones
2. Tablets

Embedded Devices

1. Network Attached Storage
2. VMware vSphere Hypervisor (ESXi)
3. Building control and monitoring systems
4. Multimedia and video conferencing equipment
5. Point of sale devices
6. Building access control, vending, and laundry devices
7. Time clocks
8. Security cameras
9. Game consoles
10. Printers and multi-function devices
11. Linux Workstations
12. Other devices running embedded operating systems

Guest Devices

Guest devices include any workstation or smart device brought to campus by a guest of the University. Guests are not permitted to connect servers or embedded devices to the network.

IRM-3001.2 – Policy

Information Services provides campus network connectivity to faculty, staff, students, guests, volunteers and contractors in order to facilitate the educational mission of the institution. Network connectivity can take the form of a wired connection, wireless connection, or remote access connection via the campus VPN.

All network-connected devices must be connected to switches, wireless access points, and VPN devices that have been configured and deployed by Network Services. No third party or departmental network access equipment is permitted without prior written approval from Network Services (network@richmond.edu).

It is important that the requirements in this policy are evaluated prior to the purchase of any network-connected device. In order to protect the integrity of the network and the various people, systems, data and devices that are attached, Network Services reserves the right to deny access to the network if a device does not meet the requirements specified below. In all cases, users of the campus network are always required to adhere to the requirements outlined at http://is.richmond.edu/policies/index.html

For the purpose of this policy, network-connected devices are divided into classes, with a different set of requirements applying to each class.

Device Requirements

Workstation Requirements

1. Workstations must support DHCP. Manually configured or static addresses are not supported. Workstations that require an unchanging assigned IP address may be supported via DHCP reservations if Network Services deems appropriate.
2. The workstation operating system must be patched on an automated basis to guard against security vulnerabilities.
3. University approved anti-virus software must be installed and be configured to automatically update. Please see information at http://is.richmond.edu/get-connected/protection/index.html.
4. University approved anti-malware software must be installed and configured to automatically update. Please see information at http://is.richmond.edu/get-connected/protection/index.html.
5. A host firewall must be configured to disallow all inbound connections.
6. Wireless workstations should be configured to connect to the “urwin” encrypted wireless network via WPA2 Enterprise 802.1x authentication.

Server Requirements

1. Server administrators are responsible for the maintenance of their servers. This includes patching, troubleshooting, and sometimes rebooting.
2. Server documentation must be provided to Network Services (network@richmond.edu) so that the impact of the server on the campus network can be assessed. Documentation must include what other endpoints on the network the server will communicate with and what protocols and ports will be used
3. The server operating system must be patched on at least a quarterly basis to guard against security vulnerabilities.
4. Servers must be configured to authenticate end users to a central password store such as Active Directory, OpenLDAP, or MIT Kerberos. This requirement may be waived if the number of end users is five or less.
5. If the server contains user data, backups should be configured and scheduled to occur in accordance with University standards. Please see information at https://is.richmond.edu/policies/computer-systems-backup.html.
6. The server will be scanned with Nexpose security software periodically. Any vulnerabilities found will be remediated by the system owner within 30 days.

7. A host firewall must be configured to only allow those inbound connections that are required for the server to function as designed.

Smart Device Requirements

1. Smart device owners are responsible for the maintenance of their devices. This includes patching, troubleshooting, and sometimes rebooting.
2. Devices must support DHCP. Manually configured or static addresses are not supported.
3. Wireless devices should be configured to connect to the "urwin" encrypted wireless network via WPA2 Enterprise 802.1x authentication.

Embedded Device Requirements

1. Embedded device owners are responsible for the maintenance of their devices. This includes patching, troubleshooting, and sometimes rebooting.
2. Devices must support DHCP. Manually configured or static addresses are not supported. Devices that require an unchanging assigned IP address may be supported via DHCP reservations if Network Services deems appropriate.
3. Device documentation must be provided to Network Services (network@richmond.edu) so that the impact of the device on the campus network can be assessed. Documentation must include what other endpoints on the network the device will communicate with and what protocols and ports will be used.
4. When possible, wireless devices should be configured to connect to the "urwin" encrypted wireless network via WPA2 Enterprise 802.1x authentication. If WPA2 Enterprise is not supported, the device may be registered and permitted to connect to the MAC authenticated "Richmond" unencrypted wireless network.

Guest Device Requirements

1. Guest device owners are responsible for the maintenance of their devices. This includes patching, troubleshooting, and sometimes rebooting.
2. Devices must support DHCP. Manually configured or static addresses are not supported.
3. Devices should be configured to connect to the MAC authenticated "Richmond" unencrypted wireless network.

Exceptions and Enforcement

Any device found to be connected to the network and in violation of this policy may be disconnected without notice. Device owners may apply for exceptions to this policy by submitting a request to Network Services (network@richmond.edu) in writing.

IRM-3001.3 – Applicable Regulations and Accreditation Standards

SACSCOC *Principles of Accreditation* 10.6 (Distance and Correspondence Education)

RELATED POLICIES:

POLICY BACKGROUND:

Policy created on November 18, 2016

POLICY CONTACTS:

Vice President for Information Services & Chief Information Officer
Assistant Vice President for Systems & Networks