UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-3001	**Policy Title:**	Network Device Connectivity Policy
Effective:	07/01/2021	**Responsible Office:**	Information Services
Date Approved:	06/29/2021	**Approval:**	Vice President for Information Services & Chief Information Officer
Replaces Policy Dated:	11/18/2016	**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:

POLICY STATEMENT:

IRM-3001.1 – Purpose

The University of Richmond provides network connectivity to faculty, staff, students, and visitors to facilitate the educational mission of the institution. Network connectivity can take the form of a wired connection, Wi-Fi connection, or remote access connection via the campus VPN.

Devices that connect to the Campus Network must satisfy minimum network security requirements to protect the integrity of shared data, systems, and operations. Devices that cannot be meet these requirements may be permitted to connect to the Restricted Network. A Visitor Network is provided for anonymous Wi-Fi access for those not affiliated with the University.

IRM-3001.2 – Definitions

University Networks

Campus Network

The Campus Network is the primary point of access for faculty, staff, and students to the University's computing resources, systems, and data.

Restricted Network

University assets that do not meet the minimum network security requirements may be connected to the Restricted Network. The Restricted Network is comprised of devices that would normally pose a vulnerability to other users, data, and applications. The Restricted Network allows aging technology to continue to run on a short-term basis, until it is upgraded or replaced, by restricting the ability of devices to connect to services on the Campus Network.

Visitor Network

The University provides an anonymous and unencrypted Wi-Fi network for visitors. There may be some restrictions regarding access to University and Internet resources on the Visitor Network.

Classification of Networked Devices

Workstations

Workstations are general use devices that run Microsoft Windows, macOS, or Linux operating systems.

Servers

Servers are devices that provide shared resources such as file shares, printers, or an application to one or more users over the network. With very few exceptions, they can be found in the campus data center.

Smart Devices

A smart device is typically a general-purpose computing device that has multiple functions, but unlike a traditional desktop or laptop, it is usually much smaller and more mobile.

Embedded Devices

An embedded device generally contains a special-purpose operating system. The device is typically dedicated to a small set of tasks and is usually "headless" meaning there is no person directly operating the device.

IRM-3001.3 – Policy

All networks (Campus, Restricted, and Visitor) must be comprised of switches, Wi-Fi access points, and VPN devices that have been configured and deployed by Network Services. No third party or departmental network access equipment is permitted.

In all cases, users of University networks (Campus, Restricted, and Visitor) are always required to adhere to the requirements of the Acceptable Use Policy (https://is.richmond.edu/policies/acceptable-use.html), as well as those policies outlined at http://is.richmond.edu/policies/index.html.

Campus Network

The Campus Network is designed with logical and physical segmentation. Technical controls are applied to groups of users and systems to ensure data confidentiality, integrity, and availability. Security controls are placed on many shared access segments to mitigate the spread of malicious traffic. The Campus Network requires some form of authentication. Anonymous access is permitted only on the Visitor Network.

It is important that the requirements in the accompanying **Network Device Connectivity Standard** are evaluated prior to the purchase of any network connected device. In order to protect the integrity of the Campus Network and the connected users, systems, data and devices, Network Services reserves the right to remove any device from the Campus Network that does not meet the requirements or to move it to the Restricted Network.

Network connected devices are divided into classes, based on the definitions in this policy. These devices must meet the network security requirements enumerated in the **Network Device Connectivity Standard**.

Restricted Network

The following categories of workstations and servers must use the Restricted Network:

- Systems with obsolete operating systems or hardware for which patches for security vulnerabilities are no longer available from the manufacturer or vendor
- Systems that are not actively managed to install manufacturer-provided security patches in a timely manner
- Systems attached to obsolete equipment that preclude the patching of the system.

Users recognize that the devices on the Restricted Network are there because the devices represent a risk to the Campus Network. Note that these devices also represent a risk to other devices in the Restricted Network. Any unusual activity or disruptions should be reported to the Help Desk.

Restrictions for devices on the Restricted Network are documented in the **Network Device Connectivity Standard**.

Visitor Network

Faculty, staff, and students should not connect devices to the Visitor Network. Visitor devices include any workstation or smart device brought to campus by a visitor of the University. Visitors are not permitted to connect servers or embedded devices to the Visitor Network. Connectivity to the Visitor Network does not require authentication.

Restrictions for devices on the Visitor Network are documented in the accompanying **Network Device Connectivity Standard**.

IRM-3001.4 – Applicable Regulations and Accreditation Standards

SACSCOC Principles of Accreditation 10.6 (Distance and Correspondence Education)

Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

General Data Protection Regulation (GDPR) (EU) 2016/679F. Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Public Law 106–102, 113 Stat. 1338

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191

Payment Card Industry Data Security Standard (PCI DSS)

SACSCOC Principles of Accreditation 12.5 (Student Records)

RELATED POLICIES:

IRM-4003 Information Security Policy

IRM-2001 Acceptable Use Policy

POLICY BACKGROUND:

Policy created on November 18, 2016
Revisions to policy reviewed by President's Cabinet on 06/28/2021 and approved by VP & CIO on 06/29/2021

POLICY CONTACTS:

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