

Roger Williams University

VPN Remote Access Policy

Purpose

A remote access Virtual Private Network (VPN) service is needed to access computing resources hosted at Roger Williams University (RWU) while working remotely. The purpose of this VPN policy is to provide guidelines to access IT services hosted at RWU. This policy is based on security best practices to ensure the confidentiality, integrity, and availability of RWU digital assets.

Scope & Guidelines

This policy applies to all RWU faculty, staff, and 3rd party contractors that require remote access to RWU's private network infrastructure.

- Only established RWU.EDU faculty, staff, and administrative accounts are allowed.
- Temporary, shared, and student accounts are not permitted.
- Vendor (AKA 3rd Party) accounts may have remote access under special approval: vendor accounts must have an RWU employee/department sponsor. The RWU sponsor bears responsibility for the vendor account. If the vendor account does not exist, the department sponsor must submit a [request form](#).
- BYOD (bring your own device) is permitted remote access under special approval and conditions disclosed in RWU's **BYOD Policy**. By using VPN technology with personal equipment, users must understand that their devices are a de facto extension of RWU's private network and, as such, are subject to security rules and regulations that apply to RWU-issued devices.

Policy

- VPN access is managed by the RWU-IT department, including DNS filtering and log monitoring.
- All devices with remote VPN access are subject to **RWU's Acceptable Use Policy**.
- Remote devices may use only VPN client software issued by RWU-IT.
- VPN sessions require multi-factor authentication (MFA).
- VPN access is terminated immediately after network sessions ends.
- Data security: remotely processing sensitive and restricted data elements must comply with RWU's **Data Storage Policy**.

Procedures, Requirements, and Responsibilities

- RWU-IT is responsible for implementing and maintaining the university's remote access services.
- Requests for remote access are initiated using the [Mediatech request form](#).
- Unauthorized users are not allowed access to the device equipped with remote VPN access.
- Redistribution of the RWU remote access VPN software is prohibited.
- Once connected to RWU's VPN, all routable network traffic will travel across the VPN tunnel.
- RWU does not provide remote internet access. Users are responsible for the procurement and cost of acquiring basic broadband internet connectivity.

- Technical support is provided by MediaTech during normal business hours (M-F 8:00 AM – 5:00 PM) 401.254.6363 mediatech@rwu.edu.

Restrictions and Enforcement

- VPN services are used solely for RWU business purposes.
- VPN access will be suspended following any suspicious network activity or alerts.
- Intentional violations of the remote access policy are subject to the loss of VPN privileges.

APPROVED BY” RWU-IT, 6/20/2023

Standard Number: IT.VPN.V2

Category: Remote Access

Owner: Information Technology

Effective: 6/20/2023

Revision History: 5/30/2023 Information Security Officer

Review Date: 6/20/2023