Radford University
Information Technology Services

Information Technology Policy and Procedures

Policy: Remote Access

Policy Title: Remote Access	**Approval Date: 3/1/2022**
Policy ID: 5202	**Effective Date: 7/2/2018**
Oversight Executive: Associate VP for IT & CIO	**Next Review Date: 3/1/2024**

1. Purpose

It is crucial that RU implement safeguards to protect its information resources. Remote Access refers to the ability to access RU network resources while off campus. Security measures for remote access should be implemented based on sensitivity and risk to University systems and data.

2. Policy

- A virtual private network (VPN) connection must be established during the off-site remote access of sensitive IT systems to ensure all exchanges of sensitive information are encrypted.
- Remote users connected to the Radford University VPNs will not be allowed to leverage split tunneling capabilities. Split tunneling allows for unauthorized external connections, making systems more vulnerable to attack and exfiltration of organizational information.
- All remote file transfers of sensitive data must utilize encryption including but not limited to (sftp, https, …)
- Users must request VPN authorization for remote access to sensitive systems.
- Users must follow IT standards for hardening of systems including the installation of anti-virus software and automatic updates. See standard 5214-s for additional information.
- Records logging remote connections must be maintained in accordance with the logging and monitoring policy.

3. Procedures

Radford University will maintain, at a minimum, the following VPNs to restrict access to systems with sensitive data:

DoIT VPN – Utilized by IT Infrastructure staff to administer system and network devices.
Enterprise Systems VPN – Utilized by the Enterprise Systems programming staff.
Banner VPN – Utilized by campus users needing access to sensitive systems including Banner INB and Cognos reporting. Access to this VPN is a part of the request for access to Banner INB.
General VPN – Utilized by faculty and students to connect to non-sensitive RU resources.

4. Definitions

5. Related Information

6. Policy Background

7. Approvals and Revisions

Approved: December 18, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: 10/09/09
Minor change to reference Standard 5214-s
Approved: October 9, 2009 by Vice President for Information Technology & CIO, Danny Kemp
Reviewed: July 1, 2012
No changes.
Approved: July 1, 2012 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: July 1, 2014
No changes.
Approved: July 1, 2014 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: July 2, 2018
Changed approval for DoIT VPN and other minor wording changes for clarification.
Approved: July 2, 2018 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: March 1, 2022
Added language regarding our disablement of split tunneling.
Approved: March 1, 2022 by Associate VP for Information Technology and CIO, Ed Oakes

Reviewed February 27, 2024
Minor grammatical correction
Approved March 1, 2024 by Associate VP for Information Technology and CIO, Ed Oakes