Remote Access Device Standard

Version 2.4

STANDARD INFORMATION	
This table should be completed by the responsible office(s) and IT Risk & Compliance, as it provides general information about the standard.	
RESPONSIBLE OFFICES	IT Security Office (ITSO)
ADDITIONAL INFORMATION	▪ Responsible Use of Computing (University Policy Number 1301) ▪ Information Technology Security Program (University Policy Number 1311) ▪ Information Technology Security Standard (ITS.ITS-STD003)
DOCUMENT CONTROL NUMBER	ITS.ITSO-STD007
LAST REVIEWED DATE	3/14/2024
APPLIES TO	This standard applies to ITS personnel who maintains the VPN system for George Mason University.

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
2.0	6/26/2018	IT Security Office	Updates
2.1	1/10/2020	IT Security Office	Annual Review; Minor Revision (reformatting)
2.2	2/15/2021	IT Security Office	Annual Review; Minor Revision (reformatting)
2.3	03/16/23	IT Security Office	Annual Review; Minor Revision (reformatting and minor clarifications)
2.4	3/14/2024	IT Security Office	Annual Review; Minor revisions to the definitions of virtual private network and remote access software have been made, along with clarification of standard requirement 4. Added exception statement.

ABOUT THE STANDARD

PURPOSE

This document lists the standards used to support the University's VPN system.

DEFINITIONS

ACRONYM/TERM	DEFINITION
Remote Access software	Examples include RDP and SSH: RDP is a remote access communications protocol available on MS Windows operating systems. Secure Shell is a remote access protocol typically used with Unix/Linux based operating systems.
Virtual Private Network (VPN)	VPN is a remote access service that creates a secure tunneled connection between an internet user and a trusted network. A VPN is used to provide an additional layer of security for remote access or to provide a presence on an internal network.

STANDARDS

All remote access gateway devices shall meet the following requirements:

1. VPN tunnels must use industry-standard strong encryption.
2. VPN must prevent split tunneling, with an allowed exception for local network access.
3. Active VPN sessions must time out after no more than 12 hours. Idle VPN sessions shall time out after no more than 60 minutes.
4. Direct remote access to internal University network devices using any method other than the university enterprise VPN is prohibited unless an exception has been submitted, reviewed and approved. Passwords shall, at a minimum, comply with the University's password complexity requirement.

EXCEPTIONS

See exceptions and exemptions section in the University IT Security Standards: IT Security Standards - Information Technology Services (gmu.edu)

TIMETABLE FOR REVIEW

This standard will be reviewed every 2 years at a minimum.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
ITSO Director	Curtis McNay	DocuSigned by: Curtis McNay 6179577EE174479...	3/19/2024
(Interim) Vice President and Chief Information Officer	Charles Spann	DocuSigned by: Charles Spann 463A1FFF579B4BC...	4/15/2024