Remote Access User 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	▪ Data Stewardship (University Policy Number 1114) ▪ 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-STD006
LAST REVIEWED DATE	3/14/2024
APPLIES TO	This standard applies to all remote access users.

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
2.0	6/26/2018	IT Security Office	Updates
2.1	12/11/2019	IT Security Office	Annual Review; Minor Revisions (reformatting, updated hyperlinks, corrected software tool name)
2.2	2/16/2021	IT Security Office	Annual Review; Minor Revisions (reformatting, revised specifics with broad terminologies)
2.3	03/16/23	IT Security Office	Annual Review; Minor Revision (reformatting and updated URLs)
2.4	3/14/2024	IT Security Office	Annual Review; Minor updates to clarify Level 2 and Level 3 Standards and DCN to reflect ownership.

ABOUT THE STANDARD

PURPOSE

The purpose of this standard is to define the user's requirements for connecting to George Mason University's network from any host. These standards are designed to minimize the potential exposure to George Mason University from damages which may result from unauthorized use of George Mason University resources. Damages include the loss of highly sensitive or University confidential data, intellectual property, damage to public image, and damage to critical George Mason University internal systems.

DEFINITIONS

ACRONYM/TERM	DEFINITION
Highly Sensitive Data	Data that (1) could lead to identity theft or exposure of personal health information if exposed, or (2) has been identified by a researcher, funding agency, or research partner as requiring a high level of security protection.
Two-Factor Authentication (2FA)	2FA service is a higher-security login process, which provides a second layer of protection to a user's identity, as well adding protection to data, systems, and services.

STANDARDS

List statement(s).

<u>Level One (Applies to students)</u>

1. Remote access by students is limited to the BYOD (Bring Your Own Device) network established by Information Technology Services (ITS).

<u>Level Two (Applies to all Mason employees and contractors requiring remote access to George Mason internal networks):</u>

1. It is the responsibility of all users with remote access privileges to ensure that unauthorized users are not allowed access to George Mason internal networks.
2. All University owned computers, which connect to George Mason internal networks via remote access technologies, must use the most current version of the centrally supported anti-malware endpoint protection software. All personally owned computer must use a current industry standard anti-malware endpoint protection software that is configured to automatically update
3. All hosts that connect to George Mason internal networks via remote access technologies must have current security patches applied to their operating systems and software applications.
4. All hosts, including personal computers, which connect to George Mason internal networks via remote access technologies must use a host firewall.
5. Two-Factor Authentication (2FA) is required to authenticate all remote access VPN sessions connecting to George Mason internal networks.

<u>Level Three (Applies only to users accessing highly sensitive data):</u>

In addition to Level Two requirements, the following applies to all users who require access to highly sensitive data and/or systems. For more information on what is considered highly sensitive data see the following website: https://its.gmu.edu/service/highly-sensitive-data/

1. All computers accessing data and/or systems classified as restricted- highly sensitive must be University owned and managed by ITS supported enterprise endpoint management systems.
2. All hosts that store highly sensitive data must utilize enterprise managed full disk encryption. Where required based upon legitimate business need the user must request and be approved to store highly sensitive data. To request the right to store highly sensitive data see: https://its.gmu.edu/service/highly-sensitive-data/

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