Remote Access User Standard

Version 2.1

Responsible Offices:

IT Security Office

Related Document(s):

University Policy Number 1114, Data Stewardship
University Policy Number 1301, Responsible Use of Computing
University Policy Number 1311, Information Technology Security Program
Information Technology Security Standards

Referenced Document(s):

University Policy 1301, Responsible Use of Computing

Document Control Number:

ITS.ITS-STD006

I. Scope

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. All remote access users are required to comply with University Policy 1301 *Responsible Use of Computing* and all other applicable George Mason University information security policies.

II. Standards

Level One (Applies to students)

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

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

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 hosts, including personal computers, which connect to George Mason internal networks via remote access technologies, must use the most current version of the centrally supported anti-virus program for specific operating systems.
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.

Level Three (Applies only to users accessing highly sensitive data):

In addition to Level Two requirements, the following apply 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/working-with-its/it-security-office/highly-sensitive-data/

1. All hosts must be University owned systems; all Windows and Mac hosts must be centrally managed by ITS via MESA Active Directory Environment for Windows system and JAMF Pro for Apple Mac OS or IOS.
2. All hosts that store highly sensitive data must enable full disk encryption and the user must have explicit permission to store the data. Contact the ITS Support Center to request permission to store highly sensitive data: https://its.gmu.edu/knowledge-base/how-does-someone-begin-the-process-of-obtaining-authorization-to-store-highly-sensitive-data-hsd/

III. Definitions

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.
JAMF Pro	JAMF Pro is a software tool for managing Mason-owned Macs that enables ITS to inventory hardware, distribute software and fixes, improve security, and get a better understanding of the Mac community at Mason.
MESA Active Directory Environment	The MESA Active Directory Environment provides for patching, security configuration and access control for Mason-owned computers running on Microsoft Windows MUST be joined to the MESA active directory system. This system enables ITS to inventory hardware, distribute software, improve security for these computers.

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.

IV. Compliance

All ITS employees are required to abide by this standard and follow the processes/procedures, if applicable. Issues of non-compliance will be referred to the Vice President and Chief Information Officer, Information Technology Services and may result in disciplinary action.

V. Dates

A. Effective Date:

This standard will become effective upon approval.

B. Date of Most Recent Review:

2/5/2020

VI. Timetable for Review

This standard and any related documents, if applicable, shall be reviewed annually or more frequently as needed.

VII. Signatures

Approved:

_____ _____

Executive Director/Chief Information Security Officer — Date
Information Technology Services

_____ _____

Vice President and Chief Information Officer — Date
Information Technology Services

Revision History

Date	Version	Purpose of Revision
6/26/2018	2.0	Updates
12/11/2019	2.1	Minor Changes- 1. Reformatted content on the new ITS Standard Template; 2. Updated version number and included additional signatory requirement to comply with ITS.ITS-PROC001, Development, Review, and Revision of ITS Documentation Procedure 3. Updated current version of software tool name from JAMF to JAMF Pro 4. Updated hyperlinks 5. Updated Level 3 requirements by updating how Mason-owned computers are centrally managed by ITS.