George Mason University	*ITS Standard* **Remote Access User**
Version 2.0	*Date of last revision: 06/26/2018*

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.

User Requirements:

Level One (Applies to students)

1. Remote access by students is limited to the BYOD (Bring Your Own Device) network established by 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:

http://itsecurity.gmu.edu/resources/highly-sensitive.cfm

1. All hosts must be University owned systems; all Windows and Mac hosts must be centrally managed by ITS via SCCM or Jamf.
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://itservices.gmu.edu/help.cfm