George Mason University	*ITU Standard* **Remote Access User**
Version 1.0	*Date of last revision: 09/16/2011*

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.

User Requirements:

Level One (Applies to all remote access users):
The following apply to all users who require 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 are connected 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 are connected to George Mason internal networks via remote access technologies must have current operating system security patches applied.
4. All hosts that are connected to George Mason internal networks via remote access technologies must have current security patches applied for common applications such as, but not limited to, Adobe Acrobat, Adobe Flash, Microsoft Office, and all web browsers.
5. All hosts, including personal computers, which are connected to George Mason internal networks via remote access technologies, must use a personal host firewall.

Level Two (Applies only to users accessing highly sensitive data):
In addition to Level One 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://security.gmu.edu/hsdfaqs.html

1. All hosts must be University owned systems.
2. All hosts must use the ITU SSL Virtual Private Network (VPN) for remote access. The Staff/Faculty VPN Request Form can be found here: http://tsd.gmu.edu/net/Forms/F0021_A.html
3. All hosts that store highly sensitive data must have full disk encryption enabled and the user must have authorization to store the data. Requests to store sensitive data are initiated at the following website: https://hsd.mesa.gmu.edu/