Remote Access Policy
USG Policy 6 (3.50) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

This policy is provided to define standards for accessing campus information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

The scope of this policy covers all employees, contractors, and external parties that access non-public USG resources over a third-party network, whether such access is performed with USG-provided or non-USG-provided equipment.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Modem*: a hardware device that allows a computer to send and receive digital information over a telephone line.

B. *Remote Access*: the act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

C. *Timeout*: a technique that drops or closes a connection after a certain period of inactivity.

III. Prohibited Actions

A. Remote access to USG systems is only to be offered through a USG-provided means of remote access in a secure fashion. The following are specifically prohibited:

1. Installing a modem, router, wireless access point, or other remote access device on a USG system without the approval of the OIT Director.
2. Remotely accessing USG systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the OIT Director.

IV. Remote Access Tools and Screen Sharing

A. Many video conferencing and web meeting applications also contain features to allow remote access and screen sharing. While these applications are not prohibited the following guidance applies:

1. Users must use institutionally provided and approved applications when engaging in a screen sharing and/or remote control of a USG system. Any exceptions must be pre-approved by the OIT Director.

2. Users who engage in screen sharing must take precautions to protect non-public USG information and system access consistent with the USG Data Classification Policy 6 (2.10). Users should only share information that is pertinent to the objectives of the shared session.

3. All remote-control sessions must be actively monitored by the granting user. This user is responsible for all actions untaken by the remote user and any resulting consequences.

V. Use of Non-USG Provided Machines

A. Accessing the USG network through home or public machines can present a security risk, as USG cannot completely control the security of the system accessing the network. Use of non-USG-provided machines to access the USG network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

1. It has up-to-date antivirus software installed

2. Its software patch levels are current

3. It is protected by a firewall

B. When accessing the network remotely, users must not store confidential information on home or public machines, see USG Confidential Data Policy 6 (2.00).

VI. Client Software

A. USG will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in accordance with USG’s Encryption Policy 6 (2.20) in order to protect the data during transmission.

VII. Network Access

A. There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

VIII. Idle Connections

A. Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to USG's network must be timed out after 1 hour of inactivity. Exceptions may be granted by the OIT Director and must be documented.

IX. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

X. Revision History

Date	Description	Revised By
07/05/2018	Initial Policy Creation	Russell Schlosburg

XI. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf