Guest Access Policy
USG Policy 6 (3.10) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

USG may wish to provide network and system access as a courtesy to guests wishing to access technical resources, such as workstations, wireless, and applications, etc. This policy outlines the USG's procedures for securing guest access.

The scope of this policy includes any visitor to the USG wishing to access the campus network or systems through USG's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse the USG's network.

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. *Account*: a combination of username and password that allows access to computer or network resources.

B. *Guest*: a visitor to the USG premises who is not an employee.

C. *Device*: any portable or fixed computational machine with the capabilities of transmitting and/or receiving data over a wired or wireless network.

D. *Template*: a reusable and predefined set of security access controls for authorized users to set, alter, and remove specific elements within its access control system for a subset of user accounts.

III. Granting Guest Access

Guest access may be granted on a case-by-case basis to any person who can demonstrate a reasonable need to access network and system resources, or access the Internet from within the USG campus network.

A. Acceptable Use Policy (AUP) Acceptance
Guests must indicate their agreement to USG's Acceptable Use Policy (I-1.01) before being granted access.

B. Approval

USG OIT shall establish templates for typical guest access. These templates shall be targeted to the purpose, the nature and the duration of needed access and shall have appropriate permissions and restrictions. The Director of OIT may designate USG personnel in non-OIT departments to create and manage accounts within these templates. Guest access requests which fall outside of the pre-approved templates shall require approval on a case-by-case basis by the Director of OIT or documented designee.

C. Account Use

USG OIT may assign unique guest accounts to individuals for access to campus IT resources. If these accounts are offered, they are only to be used by guests to whom they are assigned. Guests are responsible for maintaining the security and confidentiality of their assigned credentials.

D. Security of Guest Devices

Guests are responsible for maintaining the security of their devices and for ensuring that those devices are free of malware. USG OIT reserves the right to inspect devices if a security problem is suspected, but will not inspect each guest's system prior to accessing the network.

IV. Guest Access Infrastructure Requirements

A. Guest access will be logically separated based on USG's Network and Systems Security Policy 6 (3.30).

V. Restrictions on Guest Access

A. Guest access will be restricted to the minimum capabilities necessary. USG OIT will evaluate requests for additional access on a case by case basis consistent with approval requirements in section III, Letter B.

VI. Monitoring of Guest Access

USG OIT reserves the right to monitor guest access to ensure that USG's interests are protected and guests are in compliance with USG's Acceptable Use Policy 6 (1.00).

VII. 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.

VIII. Revision History

Date	Description	Revised By
11/07/2017	Initial Policy Creation	Russell Schlosburg

IX. Related Documents

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