Access Control Policy

USG Policy 6 (3.20) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to USG's network and/or systems are authenticated in compliance with USG standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of accounts and authentication standards.

The scope of this policy includes all users who have access to USG-owned or USG-provided computers or require access to USG's network and/or systems. This policy applies not only to employees, but also to partner faculty and staff, guests, contractors, and anyone requiring access to USG's trusted or hybrid network zones. Public access to USG's externally-reachable systems, such as the USG website or public web applications, are specifically excluded from this policy. Also excluded are access to the public network zone.

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. *Antivirus Software:* an application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

B. *Authentication*: a security method used to verify the identity of a user and authorize access to a system or network.

C. *Biometrics*: the process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

D. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

E. *Password*: a sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

F. *Smart Card*: a plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

G. *Token*: a small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

III. Account Setup

A. During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

1. Positive ID and coordination with Human Resources is required for USG employees. For faculty or staff from partner institutions, positive ID and coordination with the partner Program Director or designee is required.
2. A user will be granted the least amount of access required to perform his or her job function.
3. A user will be granted access only if he or she accepts USG's Acceptable Use Policy 6 (1.00).
4. Access to the network and/or systems will be granted in accordance with USG's Acceptable Use Policy 6 (1.00).

IV. Account Use

A. Accounts must be implemented in a standard fashion and utilized consistently across the organization. The two primary types of accounts are Individual and Functional IDs. Individual IDs are user accounts assigned specifically to one user. Functional IDs are user accounts associated with a group or role that may be used by multiple individuals or user accounts that are associated with production job processes (i.e. Service Accounts).

B. The following statements apply to account use:

1. Accounts must be created using a standard format
2. Accounts must be password protected; see USG's Password Policy 6 (3.40).
3. Where possible, Individual ID accounts should be used to provide accountability for administrative changes.
4. When Functional IDs are issued, the following controls should be in place:
   - Eligibility criteria for obtaining an account
   - Processes for creating and managing accounts including the process for obtaining users' agreement regarding USG's Acceptable Use Policy 6 (1.00)
   - Processes for managing the retention of user account information
5. User accounts must not be given administrator or 'root' access unless this is necessary for the user to perform his or her job function.

6. Occasionally guests will have a legitimate business need for access to the USG systems and/or trusted network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

7. Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the OIT Director or executive team, or as required by applicable regulations or third-party agreements.

V. Account Lifecycle and Termination

A. The Office of Human Resources and/or partner Program Directors must notify the Office of Information Technology when an employee is terminated, suspended, or their job role or function has changed. There must be documented processes that ensure that access rights reflect employee status, including changes in employee status. For critical systems, employees' access rights will be modified, as appropriate, by the close of business on the same day, after the employees' change of status is communicated to OIT.

VI. Authentication

A. End user systems in the non-public network zone must be configured to request authentication against the domain. If the domain is not available or authentication for some reason cannot occur, then the user should not be permitted to access the machine.

B. Infrastructure systems should take advantage of federated authentication whenever possible, although Functional IDs are permitted if necessitated by system configuration or limitations.

VII. Use of Credentials

A. At a minimum, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to USG's Password Policy 6 (3.40).

VIII. Remote Access

A. USG's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to USG's Remote Access Policy (3.50).

IX. Inactivity Lockout

A. Where technically capable, USG owned devices must automatically lock after 30 minutes of inactivity and require a password or other approved authentication technique to unlock. Additionally, users are strongly encouraged to manually lock their screens when leaving the devices vicinity.

X. Minimum Configuration for Access

A. USG strongly encourages users to install and regularly update anti-malware software, as well as other critical software, to the latest versions before accessing the network with non-USG owned equipment.

XI. Authentication Credential Transmission

A. USG services which require authentication credentials must provide for encryption of those credentials during transmission across any network, whether the transmission occurs internal to USG's network or across a public network such as the Internet.

XII. Failed Logons

A. Where system technology permits, accounts should be automatically locked or otherwise disabled after a maximum of 5 failed logon attempts. Automatic unlocking or re-enabling after a sufficient amount of time has passed is permitted.

B. Systems should be configured not to reveal which credential component is incorrect, if possible. The error can instead be as simple as "the username and/or password you supplied were incorrect."

XIII. Non-Business Hours

A. While some security can be gained by removing account access capabilities during non-business hours, USG does not mandate time-of-day lockouts owing to the nature of the academic campus.

XIV. 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.

XV. Revision History

Date	Description	Revised By
02/21/2018	Initial Policy Creation	Russell Schlosburg

XVI. Related Documents

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