Password Policy
USG Policy 6 (3.40) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to specify guidelines for creation and use of passwords.

The scope of this policy applies to all populations including, but not limited to, students, staff, faculty, contractors, vendors, and all campus visitors/guests who are provided an account on USG's network or systems. This includes third-party connections and cloud technology services.

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. *Administrative Level*: any account that has authorized access to make changes which would impact the system/service. These include, but are not limited to access to configuration settings and/or the ability to make configuration changes, account administration, and affect the availability of the system/service.

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

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

III. Password Construction

A. Consistent with USM's security standards, USG OIT mandates that all users adhere to the following guidelines on password construction:

1. Minimum password length: 8 characters
2. Passwords must contain a mix of lower and uppercase alphanumeric characters. Passwords must not consist of all digits, all special characters, or all alphabetic characters.
3. Passwords must not significantly resemble the user identifier

IV. Confidentiality

A. Passwords are considered confidential data and treated with the same discretion as any of USG's proprietary information. The following guidelines apply to the confidentiality of passwords:

1. Users must not share their passwords with others (co-workers, supervisors, family, etc.)
2. Users must not write down their passwords and leave them unsecured
3. Users must not check the "save password" box when authenticating to applications
4. USG strongly recommends users should not use the same password for different systems and/or accounts
5. Users must not send passwords via email unless encrypted in a manner consistent with USG's Encryption Policy 6 (2.20)

B. Any passwords must be stored in a manner consistent with USG's Encryption Policy 6 (2.20)

1. Users must not recycle previously used passwords when password updates are requested
2. Users are strongly encouraged not to use part or all of their username in corresponding passwords

V. Password Retries

A. Where technically feasible, systems will disable user accounts for a minimum of 10 minutes after not more than 6 consecutive failed login attempts.

VI. Password Change Frequency

A. General users must change passwords at least annually and administrative level accounts must be changed every 90 days. It is strongly recommended that all Functional ID passwords be changed at least annually, except where superseded by specialized access levels, controls, or circumstances that directly impact security of USG's assets. Where available, automated controls will enforce all password change requirements.

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
11/27/2017	Initial Policy Creation	Russell Schlosburg
02/22/2019	Add functional ID expiration	Russell Schlosburg

IX. Related Documents

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