OVERVIEW:
The CMU Password Policy establishes the position that poor password management or construction imposes risks to the security of University information systems and resources. Standards for construction and management of passwords greatly reduce these risks.

Pursuant to CMU's Password Policy, the following represent the expectations for any passwords in use or newly established at CMU. The standards below are effective on the date in the footer of this document and will remain in effect until this document is edited or replaced.

PURPOSE:
This document describes the acceptable standards for password construction and management.

SCOPE:
The requirements in this standard apply to passwords for any computing account on any university computing resource, to the user of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

STANDARD:
1. Passwords will be between 10 and 60 characters in length, with preference for use of an entire passphrase where possible. Minimum strength and complexity requirements for Global ID passwords, depending upon length, are as follows:
- Passwords of 10-11 characters in length require mixed case letters, numbers, and symbols
- Passwords of 12-15 characters in length require mixed case letters and numbers
- Passwords of 16-19 characters in length require mixed case letters
- Passwords of 20 or more characters in length do not require additional complexity requirements

2. Passwords will not consist of well-known or publicly posted identification information. Names, usernames such as the Global ID, and ID numbers are all examples of well-known identification information that should not be used as a password.

3. Passwords will be unique to CMU accounts (don't use your CMU password anywhere else).

4. Passwords will be memorized and never written down or recorded along with corresponding account information or usernames. Use of a reputable encrypted password manager is acceptable and encouraged, although extreme care must be taken to protect access to said application.

5. Passwords will not be transferred electronically over the Internet using insecure methods. Wherever necessary, secure protocols including HTTPS, FTPS, IMAPS, etc. will be used.

6. Passwords will not be transferred or shared with others unless the user obtains appropriate authorization to do so (See **Responsible Use of Computing Policy**).

When it is necessary to disseminate passwords in writing, reasonable measures will be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.

When communicating a password to an authorized individual orally, take measures to ensure that the password is not overheard by unauthorized individuals.

7. Systems will not be configured to allow user login without a password. Exceptions will be granted for specialized devices such as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only) that are separate from administrative accounts.

8. OIT personnel will, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include, but are not limited to: disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; public exposure or breach of a password.

9. Default passwords for administrative accounts will not be used.

10. Application developers will, whenever possible, develop applications that require secure protocols for authentication.

11. Applications and services should, whenever practical, use OIT's supported Single-Sign On (SSO), instead of requiring the creation of additional unique user IDs and/or passwords.

12. The use of multi-factor authentication (MFA) is required for all CMU faculty, staff, and students to access most of CMU's online services. The use of additional authentication factors for other services are recommended where available.

CONSEQUENCES AND SANCTIONS:
Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Any device, system, or account that does not meet the security requirements outlined in this standard may be removed from the CMU network, disabled, etc. as appropriate until the device or system complies with this standard.

EXCEPTIONS:
Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. Exceptions must be approved by the Information Security Office. To request a security exception, contact the CMU Help Desk.