Title/Subject: **GLOBAL ID PASSWORD POLICY**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees □ visitors ☒ contractors

Effective Date of This Revision: January 1, 2018

Contact for More Information: Office of Information Technology

□ Board Policy ☒ Administrative Policy ☒ Procedure □ Guideline

BACKGROUND:

CMU user accounts are the first line of defense against external intrusion into CMU data, systems, and networks by unauthorized individuals. Because Global IDs and their passwords are electronic access keys (or access tokens) to these data, systems, and networks, their construction and use should be carefully considered.

PURPOSE:

As noted in CMU's Data Stewardship Policy, all systems containing Protected or Restricted data must be protected from unauthorized access. This is accomplished using password-protected, unique access accounts – Global IDs. The University assigns Global IDs to its users that require passwords along with their use.

This policy lays out the basic rules governing the management of these passwords. It applies to all University-owned systems and devices, and, as noted in the Responsible Use of Computing Policy, to all systems and devices accessing University systems and Institutional Data. Some University systems may use additional or other IDs for access, where unable to work with the University Single Sign-On system, or where having more stringent requirements for system-specific, non-Global ID, user ID, and password management.

DEFINITIONS:

Single Sign-On ("SSO") means the authentication process that allows a user to access multiple applications with one set of login credentials. The University SSO uses Global ID and password as that login credential.

POLICY:

CMU passwords paired with a CMU Global ID for the purpose of accessing CMU data, systems, and networks must meet the following requirements:

1. Different passwords must be used for CMU and non-CMU accounts (don't use your CMU password anywhere else).

2. Passwords must be constructed to be difficult to guess or "crack." OIT will maintain password complexity rules designed to ensure the use of passwords meeting these "strong" characteristics (see Procedure below).

Authority: George E. Ross, President
History: New Policy
Indexed as: single sign-on "SSO"; passwords

3. As passwords verify each user as the authorized holder of the Global ID, passwords must be kept secret by the assigned user, and, per the Responsible Use of Computing Policy, must not be shared with others.

4. Passwords must be changed or reset upon first use and if shared; or if their secrecy has been violated or is reasonably suspected of having been violated (for instance, if guessed or publicly exposed/breached).

5. To protect against exposure of older versions or past use in other places or systems, passwords protecting Global IDs should be changed or updated every semester and must be changed at least once per year.

6. Passwords must not be used again without significant changes (a majority of characters must be changed).

7. Passwords must not be written down near, or stored with the devices or systems they protect (for instance, do not keep a written copy of your password with your laptop in your laptop bag, or on a post-it note with your computer or its peripheral devices).

8. Passwords must not be electronically stored in plain or clear-text format, nor transmitted in plain or clear-text formats (they must be encrypted), and should not be saved in web browsers or other non-secure or untrusted applications (for instance, if your browser asks to save your CMU password, click “no”).

PROCEDURE:

OIT has designed the guidance below to ensure that passwords created for use with the Global ID meet the requirements of this policy (see Policy, #2 above).

Passwords used to protect University systems must be strong (have complexity, including special characters, a mix of upper and lower case characters) or difficult to guess or crack, and should be 8 or more characters in length, with preference for use of an entire pass-phrase where possible. Minimum strength and complexity requirements for Global ID passwords, depending upon length, are as follows:

- Passwords must be at least 8 characters in length
- Passwords must be no longer than 29 characters
- Passwords of 8-11 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

These requirements may change over time, as technologies change and the speed of password cracking improves (requirements for minimum length without complexity will likely increase). Adding complexity to passwords where possible, regardless of length, will always make them stronger than non-complex passwords (but may make them harder to remember). Where long passwords or pass-phrases are used, password complexity is recommended, but not required. If whole sentences are used, for instance, then capital letters, spaces and punctuation, and possible numbers and other special characters may and can more naturally fit into their use. Plus, as meaningful sentences, they will be more memorable, leading to a lower likelihood of being written down and stored where used.

Many portable devices and non-standard keyboards are missing some uncommon or less-frequently-used special characters, or they make them difficult to access and enter. To accommodate these sorts of keyboards, the use of commonly or regularly-used special characters in normal-language communications (capital letters, spaces, some punctuation, etc.) is recommended, along with use of additional biometric security measures where available.

Additional factors of authentication beyond the secret password may be required in certain circumstances, or for access to sensitive or restricted data and elevated systems privileges (for instance, if the user is not physically present on University premises (remote access), or logging in as a super-user).

OIT will review these password requirements periodically to ensure alignment with current systems rules and requirements, including 1) the removal of needless complications or requirements shown to reduce the effectiveness of systems security, and 2) the addition or inclusion of technologies or tools that promote easier, accurate authentication or password use, and improve the security of systems (for instance, use of device-session biometrics like finger-print scanner and webcam pictures to login to devices, and password "strength-o-meters" to help set better and stronger passwords, etc.).

RELATED POLICIES AND OTHER RESOURCES:
Responsible Use of Computing Policy
Data Stewardship Policy
Information Security Policy
Computer Disposal Policy
Information Security FAQ

AMENDMENTS AND ADDITIONS:
The CIO may approve exceptions to this policy. All amendments and additions to this policy will be drafted by a committee convened by the CIO and will be reviewed and approved by the Provost and the President. Changes in this policy will be appropriately publicized.

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.