## 23. Global ID Password Standard

**Purpose:**
This standard sets the requirements and expectations for use and protection of the University's user accounts (Global IDs) and their passwords.

**Generally speaking**, Global IDs and their passwords are electronic access keys (or access tokens) to the University's non-public systems and data that must be protected. This standard lays out the basic rules governing the management of Global ID passwords. They must be unique to University use, difficult to guess or crack, kept secret, and changed when exposed or shared. They should also be changed periodically, to protect against exposure of older versions of them or past use of them in other places or systems. Additional requirements and advice are noted in the standard.

**Scope:**
This standard 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.

**Standard:**
**Global ID Password Standard**

1. **Global ID Password Requirements:**
    - **Passwords required:** per the Data Classification Standard, all systems containing Protected or Restricted data must be protected from unauthorized access. This is accomplished using password-protected, unique access accounts (the University assigns Global IDs to its users that require passwords along with their use).
    - **Passwords must be strong:** 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 entire pass-phrases 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

      **Please note:** 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).
      Use of password complexity is recommended, but not required, even where long passwords or pass-phrases are used. 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.

**Passwords must be kept secret:** as passwords verify each user as the authorized holder of the Global ID, passwords must be kept secret to the assigned user, and, per the Responsible Use of Computing policy, may not be shared with others.

- **Additional access factors may be required:** 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 not physically present (remote) on University premises, or logging in as a super-user).
- **Change exposed passwords:** 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).
- **Periodic password changes:** Passwords protecting Global IDs should be changed or updated every semester and will be required to change **at least once per year**, unless protected by compensating controls like additional factors of authentication.

2. **Requirements for Passwords Protecting Global IDs**

   Passwords protecting Global IDs:

   - **May not** be used as passwords on non-University sites or accounts (don't use your University password anywhere else)
   - **May not** be re-used (or used again) without significant changes (a majority of characters must be changed)
   - **May not** be blank, short, simple, or repeatedly, or easily guessed (passwords must contain a mix of non-repeating characters, must lock-out for a duration after repeated login attempt failures, and may not be identical to the account name or short or simple dictionary words)
   - **May not** contain publicly or reasonably known information about the user or system (for instance, may not be the full name of the person or system, or other easily obtained information about them)
   - **May not** be written down near nor stored with the devices or systems they protect
   - **May not** be electronically stored in plain or clear-text formats, 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.
   - **May not** remain unchanged indefinitely (or active indefinitely, if unchanged).

3. **Additional Requirements:**

   - **Review password requirements periodically**: password requirements should also be reviewed periodically to ensure alignment with current systems rules and requirements, including:
     - The removal of needless complications or requirements shown to reduce the effectiveness of systems security, and
     - 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 scanners and webcam pictures to login to devices, and password "strength-o-meters" to help set better and stronger passwords, etc.)

**Responsibility and Sanctions:**

All users of University computing resources are responsible for security, proper data stewardship (handling of Institutional Data), and the protection of University computing resources.

Failure to comply with these information security standards may represent a violation of the Information

Security policy, the Responsible Use of Computing policy, the Data Stewardship policy, and/or other applicable University policies. Violations of the Information Security Policy may result in suspension or loss of the violator's use privileges with respect to Institutional Data and CMU-owned Information Systems, and additional administrative sanctions may apply up to and including termination of employment or contractor status with the University (civil, criminal and equitable remedies may also apply).

**Frequently Asked Questions**
Refer to the Information Security Standards FAQ for additional information regarding this standard.

**References**
Administrative Policies and Procedures Manual:
https://www.cmich.edu/office_president/general_counsel/Pages/policies.aspx
Responsible Use of Computing Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03031.pdf
Data Stewardship Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03030.pdf
Information Security Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03042.pdf
Computer Disposal Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03012.pdf
About Information Security and the Office of Information Technology (OIT):
https://www.cmich.edu/office_provost/OIT/About/Pages/default.aspx

**Additional Information**
Questions or concerns related to this information security standard should be directed to CMU's CISO at 989.774.7445. Additional information can be found on the University web page at www.cmich.edu.

**Document History**
This is the second revision of this document. Finalized February 02, 2017