

UMBC POLICY ON PASSWORD-BASED CREDENTIAL MANAGEMENT

UMBC#X-1.00.03

RATIONALE

In order to provide for secure authentication to UMBC systems, and to comply with the University System of Maryland's computer security policy, UMBC is implementing the following password construction, aging, locking, and resetting procedures for all users of its enterprise authentication system. UMBC has chosen a password policy based on the practices set in NIST publication 800-63. This publication puts forth a science-based approach for password construction and aging rules allowing an institution to build a policy that best fits its business needs, and sets standards for credential revocation, change, and maintenance. Aligning our policies with this standard will allow UMBC to fully participate in various federated authentication & authorization communities, such as InCommon and the federal government's E-Authentication federation.

GUIDELINES:

Password Construction: Passwords shall:

1. Be at minimum eight (8) characters in length.
2. Must be constructed only of printable characters (alphanumeric and symbols, no spaces or control characters)
3. Must include at least one lower case character, one upper case character, and one alpha-numeric character.
4. Must contain no more than 3 occurrences of any one character.
5. Must not contain any recurring sequences of characters (minimum length of 3).
6. Must not contain any ascending or descending sequences of characters more than three characters in length. A sequence being defined as either ascii order, or orders of characters as arranged in the rows on a QWERTY or DVORAK keyboard. (e.g. strings such as "abc" or "qwe" aren't allowed)
7. All passwords will be checked against a dictionary of > 50,000 legal passwords; passwords constructed primarily of matching strings will be rejected.
8. Passwords must not contain derivatives of the user's NetID/username, Campus ID, Social Security Number, Date of Birth, or other directory information known to UMBC.
9. A minimum of three passwords will be kept in an individual's "password history"; passwords matching those in the history will be rejected.

Password Aging and Lockout:

1. After 10 successive failed authentication attempts, authentication to the specific credential will be suspended for 10 minutes.
2. A password will be "expired" (forced password change) after 8,388,608 failed authentication attempts.
3. Expiration may be implemented as a drop in the assurance level of the credential.

Password Changing and Reset:

Password changes will be done either through the MyUMBC portal (a web interface), or via the Kerberos KDC (kpasswd). The web interface is preferred, as it will give direct feedback as to what password construction rules have not been met if the credential provided fails to meet the rules described above.

Password resets due to forgotten credentials will be available via three methods. All three require an identity verification process that may vary depending on the level of assurance required by the user's association with the University.

1. OIT may collect a verified secondary email address from the user where an email message may be sent containing a one-time, expiring URL, that may be visited to initiate a password change on the behalf of the user. Depending on the level of assurance required by the user, there may be information verification procedures involved in the password reset process.
2. OIT may collect a number of secret questions and answers for the user; correctly answering these may be used as identity verification in order to initiate a credential change on behalf of the user. If a user initiates this password reset process and fails to provide the correct answers three consecutive times will result in a lockout from the password reset procedure, requiring the individual to initiate a password reset via another method.
3. Upon verification of identity by:
 - a. Government issued photo ID (drivers license, passport, etc.)
 - b. University issued photo ID
 - c. Matching photo on record with the Campus Identity Management System.
 - d. Other procedures of identity verification that meet or exceed the level of assurance given by those listed above.

OIT staff, or their designees, may initiate a password reset on behalf of the individual by issuing them a temporary password which may only be used to authenticate the user to the password changing application. At no time shall OIT staff directly modify a user's credential (e.g. resetting their actual password) unless it is necessary for debugging or troubleshooting account or system problems. In this case, OIT staff will either restore the credential to it's previous state, or, instruct the user to use one of the above described password reset procedures to recover access to their account.

DEFINITIONS:

PROCEDURE REFERENCE:

RELATED POLICY REFERENCES: NIST 800-63: Electronic Authentication Guideline
(http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

Policy Number: X-1.00.03 (formerly unnumbered)

Policy Section: Miscellaneous - IT

Responsible Administrator:

Responsible Office: Office of Information Technology

Approved by President: January 2007

Originally Issued:

Revision Date(s):