| Name of Policy: Password security policy. | THE UNIVERSITY OF TOLEDO 1872 |
|---|---|
| **Policy Number:** 3364-65-07 | |
| **Approving Officer:** President | |
| **Responsible Agent:** Vice President of Information Technology | **Most recent review date:** August 1, 2012 **Original Effective date:** November 18, 2008 |
| **Scope:** all University campuses | |

| ☐ | New policy proposal | ☐ | Minor/technical revision of existing policy |
|---|---|---|---|
| ☐ | Major revision of existing policy | X | Reaffirmation of existing policy |

(A)   Policy statement

Information technology is committed to ensuring that information technology's computing resources and infrastructure are appropriately protected through the use of appropriate password security measures.

(B)   Purpose

This policy establishes minimum requirements for university organizations and personnel regarding the proper selection, use and management of passwords.

(C)   Scope

Compliance with this policy is mandatory for all university computing systems and end users.

Information technology procurement activities will incorporate this policy and associated standards as system requirements in the procurement process.

(D)   Requirements

University information technology systems that incorporate password security measures for authentication will abide with this policy and associated standards. All university users will adhere to this policy and associated standards where passwords are used.

(1) Password standards will be based upon the results of risk assessments in accordance with The University of Toledo's "Information Security Framework." The standard will comprise a combination of password factors: length, composition, aging, lockout and history. The combination of these factors affect the level of security associated with a password. Where feasible, the University's minimum password factors for systems requiring secured access are as follows:
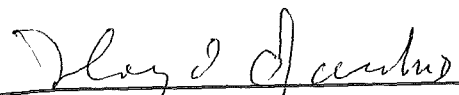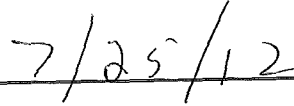
   (a) Password length: a minimum of eight characters

   (b) Password composition: contains a combination of alpha, numeric, special characters and case (upper/lower)

   (c) Password aging: a maximum password life of 180 days

   (d) Password history: a password cannot be reused within 10 iterations. Alternatively, a period of one year can be established before a password can be reused.

   (e) Password lock-out: a security action is taken after five invalid password attempts

(2) System lockout reset. Commensurate with the risk assessment of the system assets, organizations shall establish a policy on the method of reinstating a user account subject to system lockout. For systems having higher risk assets, users with a suspended account shall be re-authenticated before access is reactivated. For systems having lower risk assets, a reset feature may be used before the account is automatically reactivated, such as having a predetermined time lapse or prompting the user to provide a piece of additional information that only he or she would know.

(3) Uniqueness. When secured access is used, the combination of user ID and personal password shall authenticate a unique user. A user account for a university controlled system will be associated with a single individual and shall not be established for use by more than one person.

(4) Storage. System password files shall be maintained and safeguarded in a manner to prevent unauthorized access. Password files will be backed up to facilitate recovery from system failures, security breaches, disasters, accidents and like events with the potential to affect systems. Passwords within those files shall be stored in a one-way encrypted or hashed form and not in plain text.

(5) Transmission. Electronic transmission of passwords from one destination to another shall be protected from unauthorized access at a level commensurate with the risk assessment of the system asset. Encryption of these credentials is expected.

(6) Deactivated accounts. Accounts of employees, contractors, temporary personnel and other agents of the university who have terminated or transferred to other work units shall be deactivated. Accounts will be deactivated for such users no later than the end of business on the effective date. Accounts associated with involuntary terminations shall be deactivated immediately upon notification. The user's account may be maintained in the authentication database until all files owned by the user have been handled appropriately; at that time the user account should be deleted.

(7) Compromised accounts. Accounts compromised maliciously or by accident shall be deactivated immediately. All instances of maliciously compromised accounts shall be reported immediately in accordance with the university's security incident reporting procedures.

(8) Save password option. Organizations shall avoid system and application configurations that allow the use of save password options, except where pass-

through authentication is supported between the application and the operating system logon process. If a system's "save password" feature cannot be disabled, users shall be instructed not to use that option.

(9)  Administrative accounts

    (a)  Services and systems using system accounts and passwords or user accounts (such as administrative accounts) that have elevated access to administrative level services shall be identified and procedures developed to restrict or log their activities. Organizations shall ensure that administrators of such systems are both aware of the procedures and trained on the appropriate use of such accounts.

    (b)  Administrator groups shall be established and only authorized personnel shall be assigned to these groups. All other users shall be restricted from accessing administrator accounts. Review of the membership of these groups will be conducted semi-annually at a minimum.

    (c)  Only authorized personnel should be issued administrative accounts. Those with authorized administrative accounts shall use separate user accounts for non-system administrator tasks.

(10)  Display. Passwords shall be hidden from display at all times.

(11)  Password management. University organizations shall ensure that the management of passwords maintains confidentiality, integrity and availability. Accounts shall be permitted only for authorized users pursuant to The University of Toledo "Information Security Framework Policy."

(12)  Education and awareness. Organizations shall establish password management education and awareness efforts in accordance with university policy for "Security Education and Awareness." At a minimum, organizations shall ensure the following is addressed:

    (a)  Password protection is the responsibility of each user.

    (b)  Personal information such as social security number, meaningful dates, nicknames or other obvious information shall not constitute a password.

    (c)  A review of university policies on password composition.

(13)  Password testing. Information Technology Security personnel shall configure systems to test password effectiveness regularly if that capability is available. Password testing should be conducted by authorized personnel only and should occur at least annually. Password testing should be conducted more frequently if deemed necessary by the risk assessment defined in The University of Toledo's "Information Security Framework."

(14) Default passwords. Default application and system passwords shall be reset before deployment of any system or application. This requirement shall apply not only to conventional desktops, servers and notebook computers, but also to passwords for embedded systems, including network routers, switches and some networkable printers.

(15) Exceptions Approval. Any exceptions to these standards must be approved by the information security office in information technology.

(E)   Definitions:

(1)   Password aging. The period of time after which a password is no longer considered secure. Typically, the older the password, the less secure it is.

(2)   Password composition. The types of characters, such as upper and lower case letters, numbers and special characters that comprise a password.

(3)   Password history. Passwords shall have a re-use period commensurate with the risk assessment of the system assets being protected.

(4)   Password length. The number of characters in a password. The longer the password, the more secure it is.

(5)   Risk assessment. A process concerned with identifying, analyzing and responding to information technology security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events. See the University of Toledo "Information Security Framework" for assessment guidelines.

(6)   Save password option. An option on some systems that, when enabled, allows the user the choice of whether to have the user password memorized by the system so that it will not need to be re-entered upon subsequent access.

(7)   Source. An entity that can create or select a valid password.

(8)   System assets. Information, hardware, software and services required to support the business of the organization, and identified during the risk assessment process as assets that need to be protected in accordance with The University of Toledo "Information Security Framework."

(9)   System_lockout. A maximum number of allowed password attempts commensurate with the risk assessment of the system assets. Upon exceeding the prescribed number of unsuccessful attempts, the user account or terminal activity shall be suspended.

| Approved by: | Policies Superseded by This Policy: |
| --- | --- |
| *(signature)* | • *021, Password Management (former Health Science Campus Policy, revision date 01/ 2005)* |
| Lloyd A. Jacobs, M.D. President | • *3360-70-04, Password Policy (former Main Campus Policy, revision date 09/2002)* |
| 7/25/12 | |
| Date | |
| | Initial effective date: November 18, 2008 |
| | Review/Revision Date: August 1, 2012 |
| Review/Revision Completed by: *Vice President of Information Technology* | Next review date: August 1, 2015 |