Account Management Standard

Objective

In accordance with the Information Security and Acceptable Use Policy and to ensure authorized access and prevent unauthorized access to University Information Resources, accounts must be managed according to this standard to ensure that access to specific resources is limited to authorized users with valid need.

Centralized Authentication

When possible, computers and applications should be configured to utilize the NetID authentication system, either via Shibboleth or the LDAP protocol. Granting access via a role or membership in a security group is recommended when feasible. Default passwords present in computers and applications must be changed upon installation and must meet minimum complexity standards (detailed below).

Establishing Access

When establishing a local account (those created directly within a computer or application, not using the NetID authentication system) reasonable steps should be taken to ensure the identity of the individual receiving an account.

Access Management

Access privileges will be configured to not exceed the minimum necessary permission to perform job responsibilities. System owners are responsible for ensuring that access is authorized by the appropriate parties, is documented, and that access is removed in a timely manner when no longer required. System owners should be able to produce records of accounts including the date, time, and source of most recent login, last password change, and access assigned to the account. Access lists should be reviewed at least quarterly in order to ensure that assignments of unnecessary access are removed.

Account Expiration

When feasible, accounts should be disabled automatically unless extended based on need. For example, the account for a contractor who will be employed for 6 months should automatically disable after 6 months unless the business contract is extended.

Separation of Duties

Access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities (i.e. requesting system access while also approving one's own system access). Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated.

Password (Passphrase) Complexity

Local accounts must follow the same or stronger requirements for password complexity, password change frequency, and password re-use as the NetID system.

- Passwords must be at least 8 characters long, including the following:
  - At least one upper case letter
  - At least one lower case letter
  - At least one number
  - At least one special character
- Passwords must be changed at least once every 6 months
- Previous passwords must not be reused after being changed
- Following 10 failed password attempts, systems must lock access to the account for at least 10 minutes; preferably systems should lock access permanently until the assigned user's identity can be validated.

Password Storage

Passwords for local accounts must be stored using the strongest feasible one-way encryption method; within Microsoft Windows, use of LM or NTLM hashes is not recommended. Use of reversible encryption is discouraged.

Two-factor Authentication

In addition to a username and password, authentication may be done by other means, such as biometrics or possession of a physical device. Typically, there are three possible authentication factors:

1) Something you know, such as a password or PIN
2) Something you have, such as a mobile phone or ATM card
3) Something you are, such as a fingerprint or retina scan

Per UTS165, Two-factor Authentication will be required by August 31, 2015 in the following situations:

(a) when an employee or other individual providing services on behalf of the University (such as a student employee, contractor, or volunteer) logs on to a University network using an enterprise Remote Access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;
(b) when an individual described in (a) who is working from a Remote Location uses an online function such as a web page to modify employee banking, tax, or financial Information; or
(c) when a Server administrator or other individual working from a Remote Location uses administrator credentials to access a Server that contains or has access to Confidential University Data.

UTD has implemented a two-factor authentication solution that involves use of both a username and password, plus a device such as a mobile phone or hardware token. For more information, please see http://www.utdallas.edu/netidplus/.

Self-Service Password Reset Mechanisms

Self-service password reset mechanisms are encouraged in order to reduce workload on IT support personnel and improve the user experience. Credentials used to reset a password (such as answers to security questions) must be sufficiently specific to identify the individual, must not be predictable using social media research, and must be stored using the strongest feasible one-way encryption method. Out-of-band confirmation is preferred, such as providing a one-time password to a user's personal email address or mobile phone.

Shared Accounts

When possible, use of shared accounts should be avoided because it reduces accountability and makes it operationally difficult to change the associated passwords. For generic "root" or "admin" accounts, passwords must be changed whenever an individual who had knowledge of the password no longer requires access. Passwords for shared accounts should be securely escrowed to ensure access in the event of an emergency (viable options include use of a secure password database or storage of a password in a locked file cabinet or safe where trusted individuals may gain access to it in an emergency).

Exemptions

In the event that compliance with this standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UT Dallas President for final decision.