Account Management Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, to prevent unauthorized access to University Information Resources, accounts must be managed according to this standard. Access to University Information Resources must be limited to authorized users with valid needs to access those resources.

Centralized Authentication

When possible, computers and applications should be configured to utilize the NetID authentication system, either via Shibboleth or Active Directory. The use of these centralized authentication mechanisms reduces the complexity and risk of managing stand-alone user access systems and allows for more rapid provisioning and deprovisioning of access.

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 individual receiving an account has a current relationship with the University justifying such access. Local accounts should be named in a manner to match the NetID of the user, when feasible, to allow for easier log correlation in the future.

Access Management

Access privileges will be configured to meet the least necessary privilege required to perform current job responsibilities. Granting access to users via a role or Active Directory group is recommended when feasible and is preferable versus individual account permissions or local system accounts. When users change roles in the organization, privileges should be adjusted to match the needs of the new assignment, to avoiding accumulation of prior privileges.

A resource owner must be determined for each University Information Resource and that owner must review and approve new requests for access to the resources in their scope of responsibility. Requests to access University Information Resources may not be processed until approval from the resource owner has been obtained.

In addition to reviewing new requests for access, existing access assignments should be reviewed by resource owners periodically to ensure that access continues to be justified.

Monitoring

Event logging should be configured in a manner to allow periodic reporting of specific user account activity including the date, time, and source of most recent login, last password change, and access privileges assigned to

the user account. Further, event logs should allow reporting of all accounts that gained access to, or attempted to gain access to, a specific University Information Resource.

Changes to user access privileges, such as addition or removal of privileges and group membership, should be logged and reportable.

Account Expiration

User accounts should be disabled when no longer needed for justified business reasons. For example, if a contractor will be employed in the service of the University for 6 months, the user account provided to the contractor should be set to automatically disable in 6 months at the end of the contract period. If the business contract is extended, the user account could be re-enabled. Users accounts should not expire if currently affiliated with the University; if affiliation ends, then user access should be disabled.

Separation of Duties

Access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting operational responsibilities. Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated. When an individual has two or more roles with the University, such as an employee who also enrolls in a class, or a student who works as a parttime employee of the University, additional IT resources may be provisioned. For example, two email inboxes, to be used for the separate and distinct roles of student and employee.

Password (Passphrase)

Passwords (also defined as passphrases) for accounts should follow a security model that results that balances risk mitigation with disruption of user productivity. For example, overly complex security schemes may lead to unintended lockouts for users and disrupt their work at the University. Accounts [whether locally created through computer or application, or through the NetID system] must follow the password (passphrase) requirements:

- Minimum password length: 12 characters
- Previous passwords must not be reused after being changed (Password history: 10 passwords)
- Password complexity (using Microsoft domain method): Required
- Maximum password age: 365 days
- Lockout after failed attempts: 25
- Reset failed login attempts after: 10 minutes
- Account will be locked out for a duration of: 15 minutes

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 not recommended.

Users wishing to gain the convenience and security of an electronic password storage system may opt-in to a password database tool endorsed by the Information Security Office.

Two-factor Authentication

In addition to a username and password, authentication may be achieved 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: 1) 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;
2) 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
3) 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/.

University Information Resources containing high-risk data and/or frequently targeted by malicious actors should be protected by the NetID*plus* two-factor system, where feasible.

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. It is recommended that self-service mechanisms apply account changes immediately to reduce delay to users productivity. Out-of-band confirmation will send a one-time code to a personal email address associated with each user.

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 when someone leaves the University. For generic "root" or "admin" privileged accounts, passwords must be changed whenever an individual who had knowledge of the password no longer requires access or leaves the University. Typically, these users are members of an IT operations team. 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). Privileged accounts such as

"root" or "admin" may be set with passwords that do not automatically expire, to mitigate risk of disruption to IT services. However, periodic review and manual password changes must be performed.

To ensure that privileged accounts are not used on a full-time basis, users with a periodic need for elevated privileges should have two user accounts: a regular user account suitable for daily administrative work such as workstation login, checking email, web surfing, and editing documents, and an additional privileged account for tasks requiring elevation.

Exemptions

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

Revisions

Date	**Name**	**Changes / Notes**
April 2, 2014	Nate Howe	Started draft of Account Management Standard .
July 3, 2015	Nate Howe	First published Account Management Standard as a final document.
January 25, 2016	Nate Howe	Published revision. Specified that default passwords on computers and applications need to be changed during setup.
January 9, 2018	Nate Howe	Completed draft review and published as final. Removed expectation for permanent lockout when failures are attempted.
August 16, 2018	Nate Howe	Introduced several changes to clarify or improve wording. Also added new details, such as the allowance for a second inbox to be provisioned if justified by distinct roles at the university. Specified that LastPass, provided by UT Dallas, could be used to store passwords. Included new details about NetID*plus* two-factor protection and dual accounts for administrative work.
July 27, 2020	Nate Howe	Revised document to more clearly reflect system settings in place for the domain.