UTSA Institutional Compliance Office of Information Security

OIS 1 Account Management

I. STANDARD STATEMENT

All accounts that access university information must be managed according to access management principles as specified in this standard. The level of authorized access for an individual account must be based on the Principle of Least Privilege - that is, an individual may be granted access to only the information needed to perform the required duties.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

Commensurate with risk and reasonable practice, accounts must be reviewed regularly (preferably annually) to ensure currency of the privileges.

A. ADDITIONAL PROCEDURES FOR DATA OWNERS

1. Data Owner will inventory (with the assistance of the Information Security Administrator) software, hardware and secured facilities under his/her responsibility.
2. Data Owner will make sure there are documented procedures/processes in place for assigning, maintaining and deleting access to all owned information.
3. The ISA will prepare an Access Control List (ACL) consisting of (at minimum) names of individuals and their general level of access to resources.
4. The Data Owner (or delegate) will approve changes to the Access Control Lists.
5. The assigned ISA will maintain the inventory and ACLs for the Data Owner.
6. Data Owners will review ACLs on a regular basis (at a minimum of annually).

Title: OIS 1 – Standard for Account Management
Effective Date: August 31, 2011
Last Revised: August 5, 2020