# Computer System Access

**Original Implementation:** January 19, 1999
**Last Revision:** July 26, 2016

University information resources are strategic assets which, being property of the state of Texas, must be managed as valuable state resources. Access to university information resources is normally controlled by a login ID associated with an authorized account. Proper administration of these login IDs is important to ensure the security of confidential information and normal business operation of university managed and administered information resources.

This policy applies to university information resources that store or process mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this policy are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this policy. All exclusions must be submitted to the chief information officer for approval.

The intended audience for this policy includes, but is not limited to, all information resource owners and system administrators.

1. An approval process is required prior to granting access to an information resource. The approval process will document the acknowledgement of the account holder to follow all terms of use and the granting of access by the resource owner or their designee.
2. Each person will have a unique login ID and associated account for accountability purposes. Guest accounts are to be used in limited situations, and must provide individual accountability.
3. Access controls are to be modified appropriately as an account holder's employment or job responsibilities change.
4. Account creation processes are required to ensure that only authorized individuals receive access to information resources.
5. Processes are required to disable login IDs that are associated with individuals that are no longer employed by, or associated with, the university. In the event that authorized access is to remain active, the unit (e.g., owner, unit head) will document that a benefit to the university exists and give a date when access can be disabled.
6. Passwords associated with login IDs will comply with university password minimum requirements.

7. System administrators and other designated personnel will have documented processes:
    a. For removing the accounts of individuals who are no longer authorized to have access to university information resources.
    b. To modify user account access controls to accommodate changes in job status.
    c. For periodically reviewing existing accounts for validity.

**Cross Reference:** None

**Responsible for Implementation:** Provost and Vice President of Academic Affairs

**Contact for Revision:** Chief Information Officer

**Forms:** Account Authorization Form

**Board Committee Assignment:** Academic and Student Affairs