STANDARD OPERATING PROCEDURE

02. Creation and removal of computer accounts

Approved: 30 January 2012
Next review: 30 January 2013
Supplements: TAMU Rule 29.01.99.M1
SAP 29.01.99.M1.02
SAP 29.01.99.M1.03
SAP 29.01.99.M1.04
SAP 29.01.99.M1.14

DEFINITIONS

1. **Information resource**: The systems (procedures, equipment, and software) that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data. In the College of Architecture this includes systems such as personal workstations, networked file storage, web applications, and email/groupware services.

2. **Information resource owner**: a person or entity responsible for:
   a. a business function; and
   b. determining controls and access to information resources supporting that business function.
   In the College of Architecture an example of an information resource owner would be the Department of Construction Science, or the Business Office.

3. **Information resource custodian**: A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges. In the College of Architecture an example of an information resource custodian would be Information Technology Services (ITS).

4. **End-user**: a person who uses an information resource, usually accessed by means of a computer account, and identified by a username and password. In
the College of Architecture, both students and employees are end-users.

5. **Computer account**: Usually identified by a unique username, a computer account is the means by which end-users authenticate themselves to the information system, and the mechanism by which they are granted authorization to use that system. In the College of Architecture, each student and employee is issued an *Architecture account* that is independent of any accounts granted by the university.

**PROCEDURES**

1. **ACCOUNT TYPES**

   There are three broad classifications of computer accounts created within the college, separated by the sources that supply the account information:

   a. **Student accounts**, which are created and disabled automatically each semester based on data supplied by EIS
   b. **Employee accounts**, which are created as needed based on instructions from the college Human Resources office
   c. **Sponsored accounts**, created for guests on an as-needed basis based on requests from COA faculty or staff

2. **STUDENT ACCOUNTS**

   a. The college receives data feeds with student registration records on a regular basis from Enterprise Information Systems (EIS). This data is used to create and update student accounts at the beginning of each semester. ITS is responsible to ensure that the correct data is obtained from EIS in a timely and appropriate manner.

   b. Student accounts are created for each individual that is registered for any class taught by the college. These accounts are generated automatically, and the username is derived from the student's initials and UIN. For example, student John X. Doe with a UIN of 555001212 would be granted the username jxd1212. In case of username collisions, the second character position is converted to a digit and incremented (j1x1212).

   c. Student accounts are not created with mailbox capabilities. All TAMU
students are provided email services by CIS, and their @tamu.edu address is recorded with their account information.

d. Student accounts are always created with an expiration date set to the end of the current semester. This means that without positive action, student accounts that are created in:

   i. January (for the spring semester) expire on May 31
   ii. June (for the summer semester) expire on August 31
   iii. September (for the fall semester) expire on December 31

Expiration marks the account as inactive, and prevents activity on the account, but does not remove it. If the account remains inactive for two (2) consecutive semesters, the account is removed, and all associated data is deleted.

e. For records in the data feed that can be identified with existing student accounts, those accounts will have the expiration date moved forward to the end of the current semester, based on the same schedule used for account creation.

f. Certain resources are granted to students based on their enrollment in COA classes, and funded by student fees. These resources are tied to the student accounts, and may not be re-allocated to any other accounts that may be granted to the student for other purposes (e.g. an employee account). These resources can include:

   i. A print quota for black-and-white printing
   ii. A storage quota for the student’s home directory

g. The resources granted to students may vary based on the student’s classification; e.g. graduate students may be granted a higher storage quota or be given a longer expiration policy than undergraduates.

3. EMPLOYEE ACCOUNTS

a. There are two classes of employee accounts, separated by the classification of the employee by Texas A&M:

   i. **Non-temporary employee accounts**, which are granted to faculty and staff hired to an indefinite appointment, and contain no
account expiration date

ii. **Temporary employee accounts**, which are granted to student employees (both graduate and undergraduate) and staff or faculty on limited appointments, and are always created with an expiration date

b. Employee accounts (Non-temporary and temporary) are created based on authorization from the college HR office. Such authorization must be provided to ITS in writing before the employee account will be created.

c. Employee accounts are always created for student employees of the college, irrespective of the existence of a student account for the same individual. Because the authorization for each account arises from different sources, and because different privileges and access may be granted to the individual based on their student or employee roles, the college has elected to keep these roles separated with unique accounts for each.

d. Temporary employee accounts are always created with an expiration date. For faculty or staff, this expiration date should be the day the appointment terminates. For student employees, this expiration date will be the end of the current semester, unless the supervising manager has provided a specific date in writing to ITS.

e. ITS will send an email to all supervising managers of temporary employees 30 days before their temporary employee accounts expire. To prevent the account expiration, the supervisor must respond in writing to ITS and confirm that the individual is still employed by the college.

f. Employee accounts are deleted 30 days after they expire. ITS will send an email to the supervisor 14 days before the account removal, with instructions on how to access any data stored on COA systems that may have been owned by the employee.

g. Non-temporary employee accounts are expired and removed at the direction of the college HR office. It is the responsibility of the college HR office to inform ITS in writing within five (5) business days of any employee termination or retirement.
h. Terminated or retired employees can retain access to some college resources in special circumstances. These resources are:

   i. A college computer account with login to college computers
   ii. Access to file resources on networked file storage
   iii. Mail forwarding from a college address to an external email address

ITS must be provided a list of which resources the former employee will be granted. This list must specify a time period for this special access, include a justification for why granting the individual this access provides “a benefit to the University” (TAMU SAP 29.01.99.M1.03), and must come directly from the unit head.

4. SPONSORED ACCOUNTS

   a. Sponsored accounts are computer accounts granted to guests of the college. Sponsored accounts are created on an as-needed basis, and can be requested by any college faculty or staff employee, who will then be recorded as the sponsor for that account. Sponsored accounts are typically used to allow guests access to college resources like open access computers or classroom podiums.

   b. To create a guest account, the sponsoring employee must provide the guest’s full name, an email address, an expiration date for the account, and if the guest is affiliated with Texas A&M University, their UIN. This information must be provided to ITS in writing with at least 24 hours notice for the account to be usable.

   c. Sponsored accounts are always created with an expiration date. If a date is not provided by the account sponsor with the initial request, the account will be created with an expiration date for seven (7) days after the request.

   d. Sponsored accounts are deleted 30 days after their expiration date. ITS will send an email to the sponsor 14 days before the account is removed, with instructions on how to access any data stored on COA systems that may have been created by the guest.

5. ACCOUNT MANAGEMENT
a. Computer accounts will always require a password. This password will conform to industry best practices for complexity and expiration length. The college has elected to use the default password complexity requirements established by Microsoft for the currently implemented version of Active Directory, and has elected to match the expiration length for NetIDs used by CIS (currently 180 days).

b. Whenever possible, tools will be created to allow for self-service management of end-user computer accounts, including password resets, unlocking accounts, and editing personal information stored in the user’s profile.

c. Passwords for computer accounts can be reset at the ITS Helpdesk. The end-user must appear personally at the Helpdesk in Langford A 122, and show a valid picture ID to verify their identity. The account will be set to a temporary password, and the end-user will be forced to reset the password again upon their next login.

d. Passwords will never be reset over the phone, due to the difficulties of validating an end-user’s identity remotely.