Southern OREGON UNIVERSITY

Account Request and Closure Procedure

Office:	Information Technology
Procedure Contact:	Chief Information Officer

Revision History

Revision Number:	Change:	Date:
1.0	Initial version	05/22/2013
1.1	Format changes	03/24/2014

A. Purpose
This procedure defines the steps required to request a new account or request access changes and the process under which accounts are closed.

B. Definitions
Generic Account - An account that is intended for shared use.

Network Account - This account allows faculty, staff, and students to access university technology resources. These accounts include but are not limited to email, shared network space, and administrative systems.

Special Access Account - This account provides access to specific computer systems, including applications such as Banner, PowerFAIDS, and others.

Resource Account - These are e-mail only or calendar only accounts. They do not permit access to any other systems.

Guest Account – A network or special access account provided on a temporary basis under special circumstances to official guests, vendors, or other affiliates of the university.

C. Procedure
1. Account Creation
Network accounts for faculty and staff are created by the Department of Information Technology Department when a *Faculty/Staff New Account Request Form* is received. The following information is required to create an account: full name, SOU ID number, title, and department.

Resource accounts for departments and student organizations are created upon the request of an authorized representative of the department or organization.

Network accounts for students are created automatically by the Department of Information Technology on a daily basis. An offer of admission and acceptance is a pre-requisite for obtaining a network account for any student who does not already have an account. In certain instances, student accounts may be created prior to admission. Students who subsequently fail to enroll at the university will have their accounts removed.

Special Access accounts are created upon the request or approval of an authorized representative for the specified system. Access will only be granted as-needed and rights are restricted according to job requirements.

Guest accounts are provided only under special circumstances, such as contractual obligations, student exchanges, or other instances where there is a formalized relationship between the guest and the university. All guest account requests require the approval of the Department of Information Technology.

2. Rights Assignment and Review
Default rights given to network accounts include read/write access to personal network storage and, in the case of faculty and staff, their respective shared department folder. Only Department of Information Technology staff may change account rights or account information, other than reset passwords.

Access to administrative systems, other than access to the personal information of the account holder themselves, are granted only upon request to the Department of Information Technology and approval of the account holder's supervisor and/or other relevant persons.

An account rights review is required when a faculty or staff member changes position, job responsibilities, or department.

An account rights review is also required if a student becomes a staff or faculty member or when a student staff member terminates employment with the college.

Changes to existing rights are made upon request by authorized personnel only. All requests for changes to account rights are submitted to the department of Information Technology.

3. Employee Account Closure
a. Planned Departures
This procedure considers a planned departure to occur when a faculty or staff member has made arrangements to end their affiliation with the university at a designated future date. This process is initiated when Department of Information Technology is informed by the Department of Human Resources of an employee departure or when a *Departing Employee Information Form* is received.

i. Department of Information Technology Responsibilities

- The Computing Coordinator will assist the employee in archiving any personal electronic files, personal emails, or personal contacts if the employee desires.

- The Computing Coordinator will work with the employee's supervisor or faculty's department chair to move any university files out of the employee's personal file space.

- The Computing Coordinator will work with the employee's supervisor or faculty's department chair to retrieve any university equipment, such as a laptop, per the university's termination procedures.

- Department of Information Technology staff will reset the voicemail password at the end of business day.

- The Computing Coordinator will set the account to expire at the end of business on the designated day unless other arrangements have been made. Any other arrangements require completion of a *Departing Employee Information Form.*

- The former employee's account should be deleted within 2 business days of the employment end date. If the account is not to be deleted within 2 business days, the Computing Coordinator must note the date for deletion in the account notes field. Retention of a departed employee account past this date requires completion of a *Departing Employee Information Form.*

ii. Employee Responsibilities

If the employee wants to retain any personal files, personal emails, or personal contacts they must contact their Computing Coordinator before their employment end date if they require assistance.

b. Unplanned Departures
This procedure considers an unplanned departure to occur when a faculty or staff member's affiliation with the university is ended immediately. This process is initiated when the Department of Information Technology is informed by the Department of Human Resources of an immediate employee departure.

i. Department of Information Technology Responsibilities

- The former employee's account will be suspended immediately.

- The former employee's voicemail box password will be reset immediately.

- The former employee's account should be deleted within 2 business days of the employment end date. If the account is not to be deleted within 2 business days, the Computing Coordinator must note the date for deletion in the account notes field. Retention of a departed employee account past this date requires completion of a *Departing Employee Information Form.*

ii. Employee Responsibilities

If the former employee requires any personal files, emails, or contacts they must arrange this retrieval with their Computing Coordinator in consultation with the employee's former supervisor or faculty's former department chair. The former employee will request which items are to be retrieved. The Computing Coordinator will provide an export of the requested files, emails or contacts. The former employee must

make arrangements to pick up the materials from the Department of Human Resources.

c. Departures of Employees Who Are Also Students
If an employee departs but will remain a registered student, access to student resources needs to be retained.

    i.   Department of Information Technology Responsibilities

      –   Instead of deleting the account, all employee-related access will be removed. The account will then be converted to a student account. In some special circumstances, the former employee's account may be suspended and a new student account created instead.

      –   All other steps as above will be followed depending on whether it is a planned or unplanned departure.

    ii.   Employee Responsibilities

      –   As the account will usually only be moved, not deleted, all personal files, personal emails and personal contacts will be retained in the account.

      –   If, for some reason, a new student account was created, the Department of Information Technology will assist with migrating any personal files, emails, or contacts to the new account.

4. Student Account Closure
    i.   Department of Information Technology Responsibilities

    When a graduated or former student loses eligibility for a network account, as defined in *SOU Account Policy FAD.037*, their account will be marked for closure. After an account has been marked for closure, the account holder will receive an email notification at least two weeks prior to deletion. The notification will contain instructions about how to request the account be kept open for a limited time in case of unusual or extenuating circumstances. When the account is deleted, the account holder will lose access to all services which require a university username and password including, but not limited to, Gmail, Moodle, library databases, use of the computer labs, personal (P) drive, and personal web pages. After the account is closed, all data produced by that account (e.g. personal files, personal emails) will be permanently deleted. This process does not apply to former students who will remain employees of the university.

    ii.   Student Account Holder Responsibilities

    If the account holder wants to retain any personal files, personal emails, or personal contacts they must export this information using tools such as Google Takeout before their account is scheduled to be closed. The Department of Information Technology will provide limited support to account holders during this process, but will not perform data exports or migrations.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective

C. Associated Procedures or Other Information
Account Policy FAD.037

Collective Bargaining Agreement Oregon University System and SEUI Local 503, OPEU

SOU Computing Resources Acceptable Use Policy FAD.038
http://sou.edu/policies/Computing-Resources-Acceptable-Use.pdf

SOU Information Security Policy FAD.040 http://sou.edu/policies/Information-Security.pdf