.

OIT User ID & Account Policy

Explanation of Policy & Process Flows

Doc #: N/A, Released v1.1

Office of Information Technology

TABLE OF CONTENTS

1. Introduction

1.1. Overview

Access to Seattle University (SU) computing resources of all types is controlled by each user being assigned a User ID (userid) and then having accounts built to access various computing resources such as Microsoft Windows, UNIX, and Email as required. All personnel are covered by this policy including (but not limited to) Jesuits, faculty, staff, vendors, and students.

The objective of this document is to outline the process flows for obtaining a userid and accounts when people enter the SU community and the process flows for terminating the userid and associated accounts when people leave the SU community. People in different roles will have different requirements. In addition, there are some rules and standards that need to be put in place and explained with respect to userid and account naming, userid/account retention, and so on.

Please note that this policy is addressing the goal of how the processes *should* be followed, not necessarily how the processes actually work today. Processes outside of the control of the Office of Information Technology (OIT) are not specifically documented.

1.2. Tactical Issues

The implementation of this policy will require the cleanup and resynchronization of Colleague and Windows Active Directory (AD) databases. The most correct data is currently split across these two databases and potentially others as well. The appropriate data imports need to be done so that Colleague becomes the single primary reference database. On the Windows AD side, many thousands of userids and accounts from years past have never been disabled or deleted. Using the most current data from Colleague, userids and accounts for persons no longer associated with SU will need to be disabled and then deleted.

Beyond that, some tactical process changes need to be made so that all changes to userids are made in Colleague first and then flow from Colleague to Windows AD. No more “bypass” processes. This is an immediate change for several processes today. This will prevent the two databases from going out of synchronization while strategic process improvements and re-engineering occur at a higher level.

1.3. Items Outside Of Scope

With each userid and account, there are a number of privileges that can be acquired to access systems above and beyond the basic “birthright” services. These privileges can be acquired based on a person’s role at SU, participation in various groups, taking a specific course, etc. The details of how to acquire these additional privileges is NOT covered, but the removal of such privileges upon leaving SU is specifically covered in the process flows shown in later sections.

Security of the computing infrastructure is beyond the scope of this document and is not addressed.

2. Standards

2.1. Master Database

The Colleague database is designated as the single primary reference database that contains the master copy of records for the SU community. All other databases for

accounts and userids are subordinate to Colleague. This has some immediate consequences.

- **All personnel** at SU are **required** to have a unique Colleague ID number assigned to them. This includes vendors, contractors, and temp employees. This is done because the Colleague ID number is the one truly unique key attached to each person in perpetuity.
- Organizations such as the Provost's office, the Registrar's office, and Human Resources are required to keep Colleague fully up to date.
- All changes to data such as name or userid that are contained in Colleague **must** go through the appropriate organization to be put into Colleague. The subordinate databases such as Windows AD will accept these changes from Colleague only in order to prevent the databases from falling out of synchronization.

2.2. Differences between Colleague IDs, Userids, & Accounts

There are three related items of data used to identify each person while he/she is associated with SU - Colleague ID, userid, and account(s). The explanations that follow demonstrate the uses and the differences for each identifier.

- The "Colleague ID" is a number assigned to each person as he/she enters the SU community. Colleague IDs are never reused so they are unique to an individual in perpetuity.
- A "Userid" is assigned to each person when he/she enters the SU community and deleted when he/she leaves the SU community - userids can be reused after persons leave.
- "Accounts" are generated on an as-needed basis based on the userid to generate a personal computing resource or to obtain access to specific shared computing resources. If access is required to multiple independent computing resources, multiple accounts (based on the same userid) will be generated. Some accounts are automatically built and some are generated based on the role of the person, classes being taken, etc. Accounts will be removed at the end of the need for the account (i.e., a class (or series of classes) ends or a person's role in the SU community changes). When a userid is disabled or deleted, all associated accounts will also be disabled or deleted at the same time.

2.3. Classification of People

How OIT handles accounts depends on the role of the person who will own the account. After careful consideration, three large categories are sufficient to cover the great majority of the needs. Access to various resources is defined differently for each of the three categories. Any exceptions will be handled on a case-by-case basis by the Director of the OIT Administrative Computing team. The groupings are as follows:

- **Faculty/Staff**: This is anyone who has a long-term employment relationship (six months or more), is a member of the Jesuit community, or works at SU for a company that has a long-term vendor contract with SU (e.g., employees of Bon Appetit or Collegis.)
- **Students**: All students at SU meeting the following criteria: Must be currently enrolled or have a record of an application on file at Seattle University for a future term or semester. If the potential student does not register for classes within the first ten days of the application start term, the assigned account will be disabled then deleted following the process shown in section 4.3 "Separations".

- **Vendors**: These are short-lived accounts (<6 months) for vendors working on site, temporary staff workers, etc. Vendor accounts will all be setup to automatically expire at the end of the requested duration of the account.
- **Multiple Roles**: If a person has multiple roles at SU, he/she will be given memberships and permissions appropriate for all the roles. For the purposes of categorization, his/her userid and account(s) will be treated as dictated by the highest of the roles. (i.e., if a student is also a staff member, her account(s) will be treated as a Faculty/Staff account(s)).

2.4. Userid Naming

Each person will be assigned a userid to be used as a unique identifier for access to all computing resource accounts at SU. The standard naming convention for creating userids is as follows:

- Userids are not to exceed eight (8) characters in length. This is a safeguard for legacy computing systems that either cannot handle userids longer than eight characters or they simply ignore anything beyond the first eight characters.
- Form the userid by concatenating the last name and the first initial of the first name. If length of the last name is more than seven (7) characters, truncate the last name at seven characters for a total of eight (8) characters.
  - John Doe: doej
  - Stephi Albershein: albershs
- If the userid is offensive, switch around. Form the userid by concatenating the first name and last initial. If length of the first name is more than seven (7) characters, truncate the first name at seven (7) characters for a total of eight (8) characters.
- If the userid is already taken, add a unique sequence number on the end. The portion of the userid immediately preceding the sequence number must be truncated sufficiently so that the total length of the userid is no more than eight (8) characters.

2.5. Userid Changes

Userid name changes are difficult to implement due to the number of systems that may have to be touched when a userid is changed. So, userids are changed **only** when the appropriate office (Human Resources, Registrar, or Faculty Contracts) approves a name change or if the userid assigned is considered to be offensive.

2.6. Sharing of Accounts / Userids

Accounts and userids are assigned to individuals and are the responsibility of the individual to whom they are assigned. Do not share them! Userids are used for security purposes, logging, and audit trails. If a userid has been intentionally shared, the owner will be held accountable for any inappropriate or malicious activities tracked back to the userid. If a userid is inadvertently shared, change the password(s) on ***all*** accounts associated with the userid immediately. Reporting the problem to the Office of Information Technology (OIT) helpdesk is highly recommended.

If a shared userid is absolutely required and no other workaround exists, a specific person must be identified as the owner and responsible party for use of the shared userid. The obvious caveat here is that if a shared account is used for inappropriate or malicious purposes, this person will be held accountable for the actions of others.

2.7. Account / Userid Lifetime

SU provides access to computing resources for faculty, staff, and students to accomplish their tasks while at SU. When people leave SU, access to those computing resources will be removed on specific timelines as noted in the process flows that follow later in this document. Items to be removed include userids, accounts, all computing resources tied to those accounts, and access to any shared computing resources.

The items to be removed include, but are not limited to:

- Email mailboxes.
- Network-based home directories.
- Personal web pages.
- Access to departmental shared directories.

Because of the cost of maintaining these services, SU does not provide long-term access to computing resources for former faculty, staff, or students after they leave SU.

2.7.1. Faculty/Staff Separations

Faculty and Staff userids and accounts will be automatically disabled on the effective date of termination from Seattle University. Accounts for University employees who retire will remain active for 12 months after their effective retirement date. After this time, the retired employee's account will be disabled and then deleted. (See section 4.3, "Separations", below.)

2.7.2. Student Separations

If a Student does not register for classes for 4 consecutive quarters or 3 consecutive terms and does not have an approved leave of absence (See section 2.8 "Leave of Absence from SU", below), the student will be considered separated.

Accounts for students who graduate from the University will remain active for 12 months from the date of their graduation. If the student does not register for classes prior to the end of this period the student will be considered separated.

Once a student is determined to be separated, all userids and accounts will be automatically disabled and then deleted. (See section 4.3, "Separations", below.)

2.8. Leave Of Absence from SU

There are many reasons for faculty, staff, and students to take time away from SU. The appropriate approving organizations (Provost's Office, Human Resources, or the Registrar's Office) are required to keep information on leaves of absence up to date in Student Information System and the Human Resources System respectively.

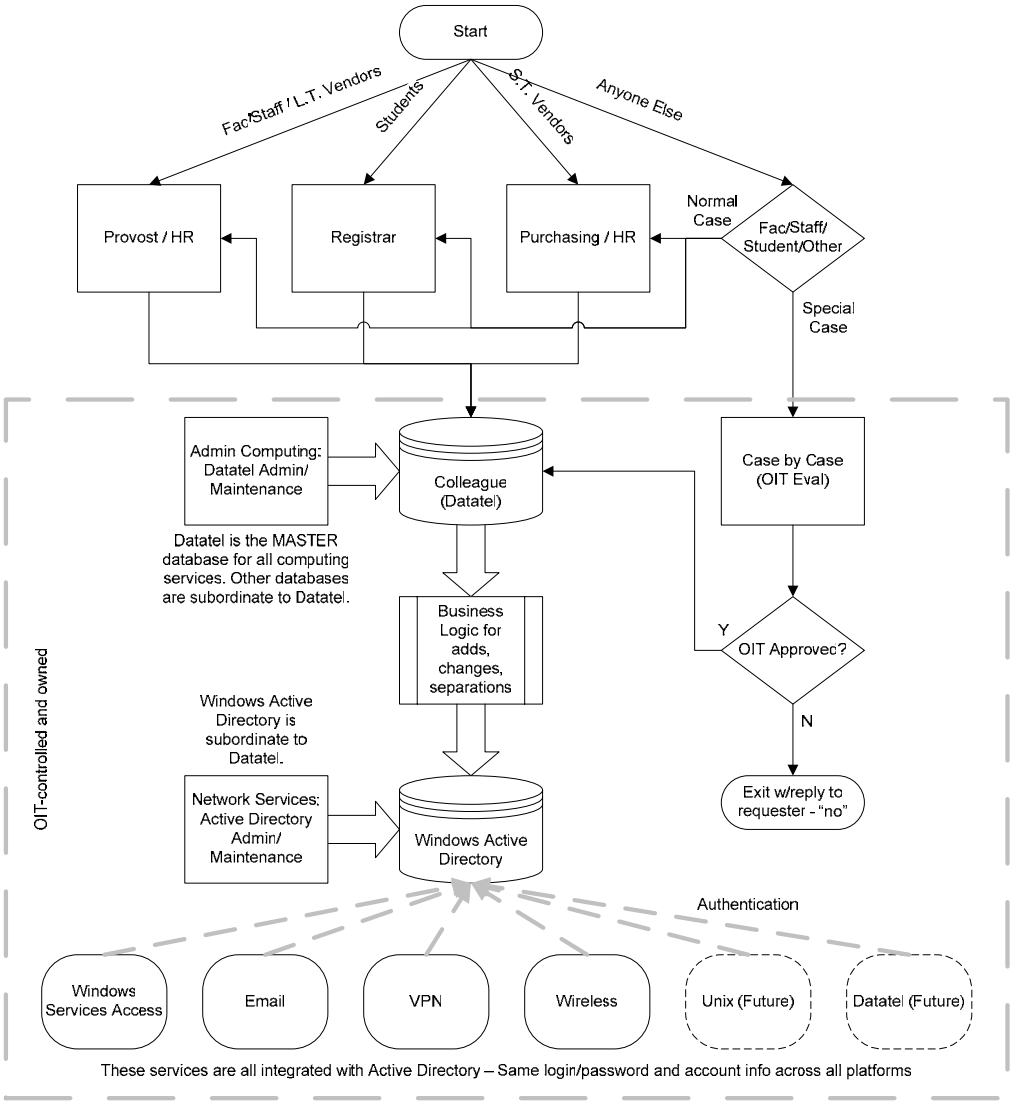
For faculty and staff, a leave of absence is not considered a separation from SU and all accounts will be maintained.

Userids and accounts for Students who receive a formal leave of absence from the Registrar will be maintained until expiration. If the student does not register for classes prior to end of this period, userids and accounts will be automatically disabled and then deleted. (See section 4.3, "Separations", below.)

3. High Level Process Flow

The data flowchart below describes what happens when a person enters the SU community. The appropriate organization enters the requests. The end result is a userid for him/her being assigned and any appropriate accounts being created and tracked in Colleague and Windows Active Directory. (L.T. = Long Term, S.T. = Short Term.)

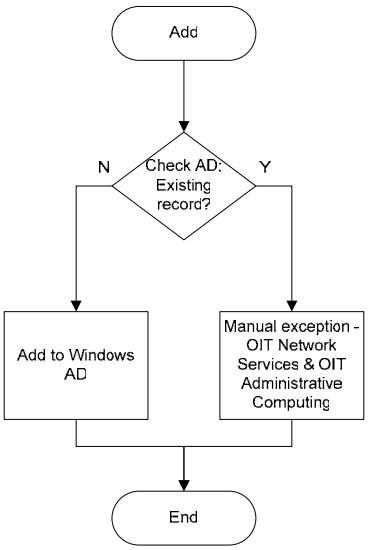
The services along the bottom of the flowchart all utilize Windows Active Directory for authentication and/or account information.



4. User: Adds, Changes, Separations

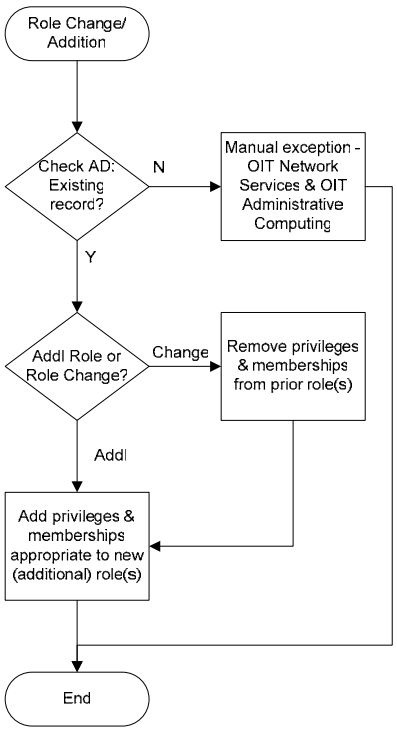
4.1. Add

Once a new user is processed through Colleague, follow the flowchart below to add a record to Active Directory.



4.2. Role Change/Addition

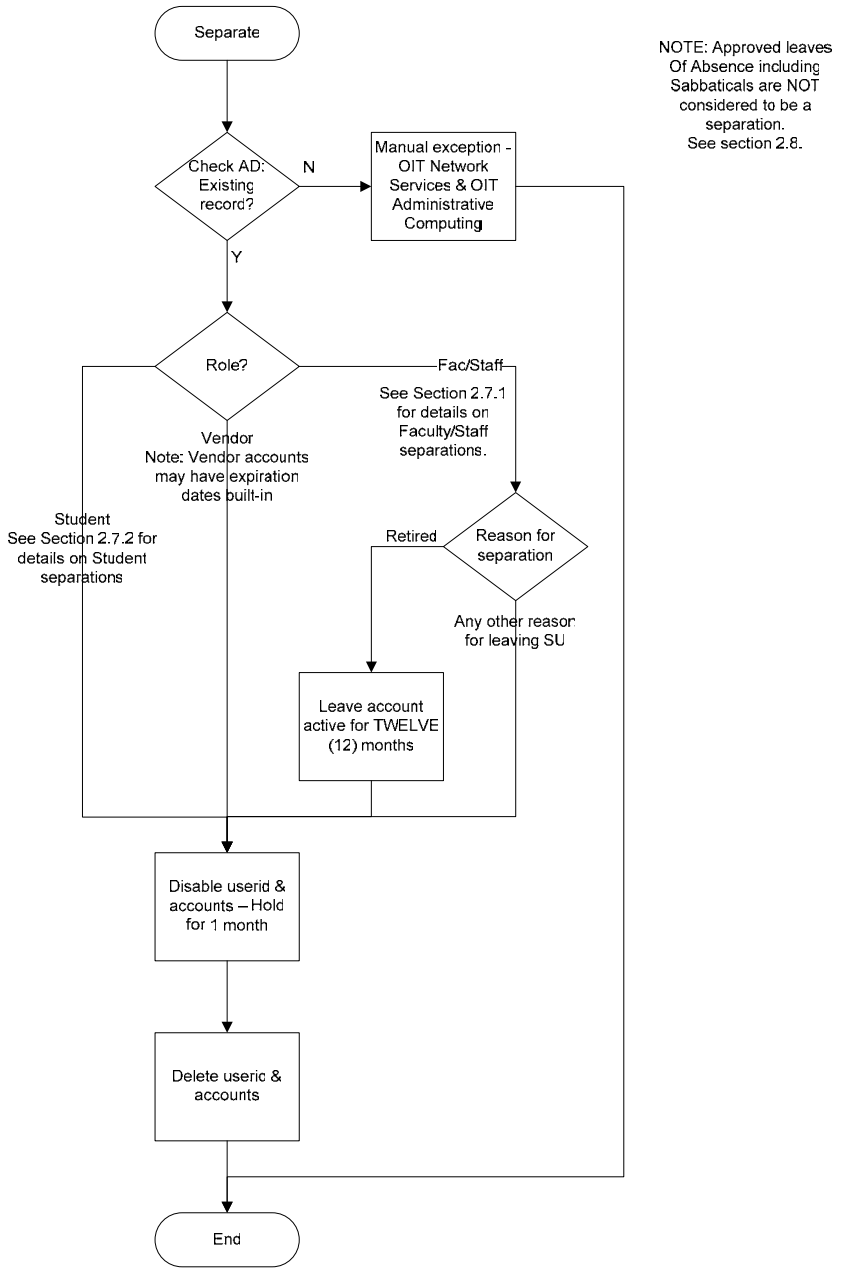
Once a change of role or addition of a new role for a user is processed through Colleague, follow the flowchart below to add/change the Active Directory memberships and privileges to be appropriate to the new role (or roles).



If person has multiple roles, they will have the sum total of the privileges appropriate for each of the roles

4.3. Separations

Once a separation is processed through Colleague, follow the flowchart below to start the process of removing the userid and accounts from Windows Active Directory (and any other related systems).



5. REVISION HISTORY

Revision	Date	Author	Description
D 0.1	9/26/2003	Hernandez	Review Draft.
D 0.2	10/28/2003	Hernandez	Review Draft #2.
D 0.3	10/29/2003	Hernandez	Review Draft #3 – Changed account retention times.
D 0.4	1/7/2004	Hernandez	Review Draft #4 - Added in most of Catherine's changes plus some of my own.
1.0	1/29/2004	Hernandez	Release copy.
1.1	6/1/2004	Hernandez / Sullivan	Release copy with clarifications to address separations. Additional minor cleanup as well.