

Computer and Information Systems Policies, Procedures, Plans and Standards

Computer User Account and Resource Policies

Effective Date: July 1, 2003
Last Update: October 7, 2009

Contents:

1.0 Purpose/Introduction

2.0 Definition of Accounts

- A. Conditions of Use
- B. General Computer/Network User Accounts
- C. Special Access/ Privileged Use Accounts

3.0 SPU Account Eligibility

- A. Account Creation and Deletion: Automation via the Management of Accounts and Resources System (MARS)
- B. Account Creation and Management: End User Interface
- C. MARS Exception Process
- D. Account Eligibility Table

4.0 Password Policies and Account Security

5.0 Employee Termination Policy (Accounts and Resources)

6.0 Account Termination and Resource Purge Policies

- A. Employee and Supervisor Obligations
- B. Banner Information System Account Termination
- C. SPU User Account Termination– Account Disablement, Account Deletion, and Resource Deletion
- D. Employee Termination for Cause

7.0 Policy Exceptions and Exclusions

1.0 Purpose/Introduction

Seattle Pacific University is a Christian educational community committed to integrating faith with learning and life. The user account and resource policies outlined in this section are designed to promote clear expectations about how accounts and resources are created, about who is eligible for what, about issues of security and confidentiality, and about how accounts and resources are affected following changes in academic or employment standing.

2.0 Definition of Accounts

Each of Seattle Pacific University's information resources and systems has unique and fundamental differences in eligibility, account duration and provisions for security. Detailed definitions of the computer accounts covered in this policy are presented on the CIS Help Pages at: <http://www.spu.edu/CISHelpDesk/accountspswd/index.asp>.

2.A Conditions of Use

Requirements and conditions concerning individual responsibilities in the use of Seattle Pacific University computer accounts and resources are described in the University's "Acceptable Use Policy." All persons are expected to understand and abide by the conditions set forth therein.

2.B General Computer/Network User Accounts

Banner Information System (Banner User ID and PIN)

The Banner Information System (referred to as Banweb) is SPU's primary resource for academic, personal, and employment information. Banner is the primary, web-based, general user interface for personal student information, for academic information (both students and faculty), for employee/personnel information, and for departmental (financial) data.

SPU User Account (SPU Username and

The SPU User account provides log in identification for university owned computer systems, as well as access to network resources, such as: SPU email accounts; Blackboard; network access

Password) (wired and wireless); public Exchange folders; department network shares; and personal NetStore and WebSpace resources.

2.C Special Access Accounts

Internet Native Banner (INB)	In addition to the general access Banner user (Banweb) account, a <i>highly restricted</i> interface is provided to the Banner Information System via "Internet Native Banner." These accounts are privileged and available only to SPU employees responsible for maintaining academic, administrative, personnel and employment records.
Blackboard	The Blackboard system is SPU's on-line learning (web) resource. Most classes utilize this system in a "blended" instructional format that integrates classroom lectures with on-line resources and components. Blackboard credentials use the SPU User Account (SPU Username and Password).
EBSCO Host (Library Patron Database)	SPU library system provides portal access to the non-SPU EBSCO Host Research Database System. SPU access to EBSCO Host is managed via the Library Patron Database system. Credentials are generated from within the Banner system and managed by the Library. Additional details should be directed to the campus library staff.
ePortfolio	Instructional Technology Services maintains access to the ePortfolio system. Credentials are granted to students and employees primarily in the School of Education. Credentials for access to this resource are separate from those discussed herein, though the SPU username is typically used. Additional details should be directed to the ITS staff.
Privileged Administrative Accounts	Privileged administrative account policies are manually assigned and managed by Computer and Information Systems. Details concerning the use of privileged administrative accounts are set forth in the CIS "Privileged Account/Audit Policy" document.
LINUX/UNIX Servers	SPU maintains a number of administrative servers, each with its own, unique account configuration that is managed independently.
Guest Access Accounts	Guest accounts are managed separately under the provisions set forth in the "SPU Guest Account" policy.

3.0 SPU Account Eligibility

Seattle Pacific University computer accounts and network resources are intended for use by SPU faculty, staff and students in the performance of academic development or University business. There may also be times when access to University resources (generally by on-campus, third-party service providers) is deemed to be in the best interests of Seattle Pacific University. This section defines specific resources and aspects of account eligibility as determined by an individual's "standing."

3.A Account Creation and Deletion: Automation via the Management of Accounts and Resources System (MARS)

User account and resource creation – regardless of the specific account or resource – is governed by an individual's "standing" as recorded within the Banner Information System. ("Standing" includes such categories as *current student, current employee, former student, former employee, etc.*)

The first step in the account creation process is that the individual needs to have a record in Banner. For faculty, staff, and "exceptions," (such as employees of University contract service providers) this occurs at the onset of employment and is managed by the department of Human Resources. Banner records for students are created at the time of registration or admission to the university – and are maintained by Student Academic Services and Admissions.

Depending on a person's standing in Banner, the MARS system automatically creates, reconfigures or deletes a standard set of accounts (referred to as the "Basic Suite"), thereby affecting an individual's resource access. The Basic Suite involves creation of the user's SPU User Account and the "dependent resources:" namely, SPU email and NetStore resources (described throughout this document).

In addition to the automated capabilities of the system, MARS also provides a user interface that permits individuals to request additional resources as well as customize certain aspects of their account (such as renaming an account or configuring email forwarding). We refer to this as the "End User Interface."

3.B Account Creation and Management: End User Interface

The end user interface to the MARS system is provided through the Banner ->Computer Resources -> Manage Computer Resources menu. Persons with access to Banner may use this interface to request additional accounts and resources (such as WebSpace), to reconfigure existing accounts and resources, and to request additional account management functions such as an automated password reset.

3.C MARS Exception Process

As noted above, exceptions to a person's standing – and therefore, changes in the normal account/resource eligibility guidelines – are based upon Banner information. An exception to the normal MARS-automated process is warranted if a person does not have "standing"

as defined on the basis of student status or University employment. Generally, these exceptions are provided for on-campus, third party service providers. Initial approval for exception status should be made within the student/employees department, followed by a formal request to the appropriate University designee (Human Resources or Student Academic Services). Once approved, a record for the individual is entered into Banner and the automated account creation process is initiated.

3.D Account Eligibility Table : General Use Accounts

The following table describes eligibility rules as they apply to all University faculty, staff and students, and may be extended to those with "exception" status on a case-by-case basis.

Banner Information System (Banner User ID and PIN)	All SPU students, faculty and staff are automatically assigned a general Banner Information System account. These are accessible through the Banner web interface. Students receive a Banner User ID and PIN automatically upon registering for a class. Faculty and staff IDs are created upon contracted employment. Once an individual's personal information (academic, personnel) is entered into Banner, it remains in the system indefinitely. SPU reserves the right to modify this provision on a case-by-case basis, determined by what is deemed to be in the "best interests" of the university.
SPU User Account (SPU Username and Password)	<p>SPU User accounts are automatically created for SPU employees and matriculated students via a process (MARS) within the Banner Information System. Non-matriculated students and alumni are also eligible for SPU User accounts, although they will need to be recorded within the Banner Information System.</p> <ul style="list-style-type: none"> ▪ A Banner Information System account is REQUIRED to obtain a SPU User account. A SPU User account is REQUIRED in order for an individual to receive an email account and privileged access to other Network resources (such as the ability to log in to a SPU office or lab computer). ▪ SPU User accounts for (a) desktop computer access, (b) email and (c) NetStore are created automatically from within the MARS system. ▪ While Blackboard (On-line Learning) access is provisioned through this account, eligibility for access to course content is controlled apart from the account creation process. See "Blackboard" under Special Access Accounts (below.) ▪ WebSpace and access to special departmental folders/shares must be requested through the MARS "Request a Resource" menu. Once created, all SPU User account information is displayed via the Banner->MARS resource menu.

3.E Account Eligibility Table : Special Access Accounts

Internet Native Banner (INB)	Persons needing Internet Native Banner accounts need to be authorized for such account access by their departments, and complete training in the Federal Educational Right to Privacy Act (FERPA) which governs how the university handles personal information. If you are an employee and believe you need access to INB, please check with your supervisor to determine if FERPA training is in order, and to initiate the INB account creation process.
Blackboard	Eligibility into the Blackboard system is determined by enrollment in a class that utilizes the Blackboard integrated learning environment. Account maintenance is handled by SPU's Learning Resources - Instructional Technology Services department. Blackboard remains the one major account that is yet to be managed from within the Banner-MARS system.
Privileged Administrative Accounts	Administrative accounts are controlled by CIS.
LINUX/UNIX Servers	LINUX and NIX-based accounts are available to faculty and staff on an as-needed basis.

4.0 Password Policies and Account Security

There are a number of policies that pertain to passwords and security involved with the privilege of utilizing computer and network resources at Seattle Pacific University. Faculty, staff and students at SPU may have a variety of credentials, many of which access important, sometimes confidential University information. It is imperative that these credentials be managed with security and confidentiality in mind. Below are some general account password policies, followed by a table presenting additional rules and guidelines unique to each resource:

- 4.A It is incumbent upon each SPU faculty, staff member and student to be mindful of potential information security risks and take appropriate steps to protect University resources entrusted to them via electronic means.
- 4.B Confirmed or suspected compromises in informational security should be immediately reported to the Computer and Information Systems (CIS) Help Desk.
- 4.C Seattle Pacific University expressly prohibits the use of third-party username/password services.

- 4.D Under no circumstances should account passwords ever be disclosed or shared.
- 4.E Identical passwords should not generally be used with different accounts. For example, the SPU username and password is used for email, and the SPU username is typically used for access to the ePortfolio system. In this example, the credentials are different though they would appear to be the same based upon the SPU username convention. The password used in each case should be different, since the credentials come from different sources.

Conversely, the SPU username and password is the credential used for Blackboard and email (SPU User Account: username and password). It is not possible to manage these passwords separately as they tie to the same credential.

- 4.E Passwords should not be written down or otherwise recorded in ways that they may be easily found by an unauthorized person.
- 4.F Strong password techniques should be used. These include: not using obvious names, identities, hobbies, etc.; not using words that can be found in the dictionary; incorporating mixed-cases, numbers, letters and special characters whenever possible; and periodically changing passwords.
- 4.G The following resource-specific password policies are also pertinent:

Banner Information System (PIN)	PINs must be six characters (alphanumeric) in length. If seven (7) invalid passwords are attempted successively the account will be "locked-out" until Student Academic Services or CIS is contacted. In addition to the Banner ID/PIN combination, users must create a <i>Security Question and Answer</i> which provides account access in the event that a PIN is forgotten.
SPU User Account (Password)	Passwords must be a <i>minimum</i> of eight characters. Password history enforced: previous three (3) passwords may not be repeated. If five (5) invalid passwords are attempted successively the account will be "locked-out" for thirty minutes, or until CIS is contacted.
Internet Native Banner (INB)	Internet Native Banner passwords cannot begin with a number; and they must be a minimum of five characters.

5.0 Employee Termination Policy (Accounts and Resources)

The following section provides detailed information regarding the processes and responsibilities of University faculty, staff and their supervisors at the time of employee separation. These procedures specify the steps that will take place in the account/resource termination process, as well as detail when these activities will take place, what the former employee is obligated to do, and where institutional over-site (direct supervisor) is needed.

5.A Employee and Supervisor Obligations

- 5.A.1 Employee Notification: Approximately one week prior to the employee's scheduled termination date, the employee will receive email notification of the requirements set forth in this policy.
- 5.A.2 Supervisor Notification: Approximately one week prior to the employee's scheduled termination date, the direct supervisor will receive email notification of the requirements set forth in this policy.
- 5.A.3 Employee Obligation of Disclosure: The employee is obligated to disclose to the supervisor all privileged information such as key contacts, email addresses, and phone numbers, files and archives etc. relevant to the functions/business responsibilities held on behalf of the University.
- 5.A.4 The employee and supervisor shall review information stored on the desktop computer and either copy files to the appropriate backup, or make sure critical institutional data is maintained. All "personal" information needs to be removed from the computer.
- 5.A.5 The departing employee's access to the computer will be removed in accordance with the timelines for disablement of the employee's SPU User Account as described in Policy 5.C.

5.B Banner Information System Account Termination

Banner Information System accounts and employee related access will generally be terminated immediately following the employee's last day of work. For details, please see Policy 6.A.3, below.

5.C SPU User Account Termination– Account Disablement, Account Deletion, and Resource Deletion

A person's SPU User Account controls access to desktop login, email, NetStore, WebSpace, department shares and other important business-related resources. SPU User Account termination involves two distinct steps: account "disablement" and account "deletion." Account *disablement* makes the account – and all its dependent resources – inaccessible to the original account user. The account remains in the system, however, and can be re-enabled or renamed as needed. Conversely, account *deletion* permanently removes the user's account from the system. In both of these instances, dependent resources remain accessible by a administrator until such time that each resource is manually purged. Both steps (account disablement and deletion) are accomplished automatically (via MARS) within a specified time frame (see Policy 6.D.2) following the employee's exit interview. These automated processes may be overridden through manual intervention, but only under extenuating circumstances (see Policy 7 for details.)

In addition to the specific timelines for SPU User Account disablement and deletion, the following procedures for managing the transition or removal of business information associated with specific dependent resources are to be followed by the employee and verified by the supervisor prior to the employee's final departure..

Employee Responsibilities:

- 5.C.1 The employee shall establish and enable an out-of-office greeting on their SPU email account. This greeting is to remain in effect for at least thirty (30) days following employment termination. (This 30 day period will hereafter be referred to as the "notification period.") The email account Out-of-Office greeting shall include the following information:
 - i. A clear statement that the employee is no longer an agent of the department or University;
 - ii. Follow-up contact information for the employee's supervisor, replacement, or other departmental designee;
 - iii. Optional: a personal forwarding address for email that is sent to the departing employee unrelated to University business.
 - iv. Email forwarding to a non-SPU email account is prohibited during the 30 day notification period.
- 5.C.2 During the notification period, an Outlook rule will be set up within the departing employee's mailbox to forward all incoming email to the alternate recipient (designated by the department –Policy 5.C.1.b).
 - i. At the discretion of the department, the email account may be configured to be inaccessible by the departing employee.
 - ii. At the discretion of the department, the departing employee may continue to use their SPU email account during the 30 day notification period, with the expressed understanding that the Out-of-Office greeting and forwarding rules will remain in place.
- 5.C.3 Special condition for departing employees who also have former-student standing: After the 30 day notification period, complete account control returns to their former student status.
- 5.C.4 The departing employee shall establish an Out-of-Office greeting on their telephone voice mail account. This greeting shall include those details described for email account Out-of-Office messages, as defined in Policy 5.C.1.
- 5.C.5 Following the 30 day notification period, the departing employee's account will persist for an additional 90 days, however, the employee's access to that account will be disabled (through disablement of their SPU User Account). During this time, the Out-of-Office greeting will persist as well as the alternate recipient forwarding rule.
- 5.C.6 At the end of the 90 day period (a total of 120 days following the last day of work) the former employee's SPU User Account will be deleted and the email mailbox purged.

Supervisor Responsibilities:

- 5.C.7 The supervisor shall:
 - i. Oversee the employee's creation of an email and voice mail Out-of-Office greetings as prescribed in Policy 5.C.1-4.
 - ii. Provide the departing employee with specific details as to how/ to whom future University correspondence shall be redirected (5.C.1.b) and oversee the establishment of the email forwarding rule as defined in Policy 5.C.2.
 - iii. Verify that the employee activates their Out-of-Office greeting prior to departure, and that this and the forwarding rule is tested and confirmed functional.
- 5.C.8 If it is discovered during the exit interview (Policy 5.A.3-4) the employee has important University-related information stored on a desktop computer or network resource, the supervisor must communicate to CIS the need to obtain this information prior to the 60-day resource deletion deadline. CIS is not responsible for information that is revealed "needed" after that time, nor is there any guarantee that purged/deleted information will be recoverable from tape backups or other information stores.
- 5.C.9 Access to the departing employee's Windows-dependant resources (including WebSpace, NetStore, desktop login access, access to departmental shares) shall be purged in accordance with the specific timelines noted in Policy 6.D.2
- 5.C.10 Removal from any and all departmental email distribution lists and departmental User Groups shall be terminated (manually by CIS) on or about the time that MARS removes the former employee from the automated lists.

D. Employee Termination for Cause

Seattle Pacific University reserves the right to revoke or modify any and all aspects of account eligibility, access, or notification in the event that employment of an individual is terminated for cause.

6.0 Account Termination and Resource Purge Policies

The following table describes account and resource policies for former students and employees of the University. Unless otherwise noted,

Type of Resource	Former Student	Former Employee
Banner Information System	<p>Access to the Banner Information System via Banweb continues indefinitely; student Banner data is not purged.</p> <p>Seattle Pacific University reserves the right to restrict former-student access if just cause is determined.</p>	<p>Employee Banner data is not purged; however, employee access to the Banner Information System is terminated within days of severance.</p> <p>Former-student standing: Banweb access continues indefinitely for former students employed by the University, provided that employment termination was not due to cause.</p>
SPU User Account	<p>Student SPU User Accounts persist indefinitely following the last quarter for which the student is enrolled at SPU. Access to specific dependent resources varies:</p> <ul style="list-style-type: none"> Email accounts persist indefinitely. The former student may choose to forward SPU email to a current non-SPU account, or may continue to access the account directly via the WebMail interface. Email accounts that receive no activity for a two year period may be cleaned and access suspended until the former student requests to have the resource reactivated. Access to WebSpace and NetStore resources exist for a period of 30 days following the last quarter of course enrollment. 	<p>SPU User Account access for former employees persist for up to 30 days following severance provided the employee leaves SPU in good standing. Access to specific dependent resources varies:</p> <ul style="list-style-type: none"> Email accounts persist for a grace period of up to 30 days following severance. During this period, the former employee is expected to forward any and all SPU-related messages to the proper University authority. Personal contacts should also be notified that the former employee's SPU email account will soon become inactive. Employee access to all other dependent resources will be terminated immediately upon employee severance, generally on or about the employee's last workday. SPU email and network related resources are the property of Seattle Pacific University. The University reserves the right to take ownership of the former employee's resources at any time during or following employment. Decisions on whether these resources will be purged or reassigned will be decided on a case-by-case basis. <p>Exclusions:</p> <ul style="list-style-type: none"> Former employees to have attained 'emeriti' standing may continue to utilize SPU User Account resources indefinitely, as determined on a case-by-case basis by the appropriate University authority. Former-student standing precludes the revocation of email, NetStore and WebSpace resources providing employment is terminated in good standing. In these instances, the termination/purge policies for former-student standing shall apply. SPU reserves the right to modify these provisions on a case-by-case basis, determined by what is deemed to be in the "best interests" of the university.
Internet Native Banner	Resource not available to students. Consequently, no termination policies apply.	INB access is terminated upon employee severance, generally on or about the employee's last workday.
Blackboard	Blackboard access is determined by class enrollment. If enrollment does not exist, access is not provided. Account maintenance is performed through the Instructional Technology Services department.	Resource access may include current employment classification. Other access is not generally provided.
Linux/UNIX Servers	Resource not generally available to students. Consequently, no termination policies apply.	Access to Linux/UNIX servers will be terminated immediately upon employee severance, generally on or about the employee's last workday. SPU reserves the right to modify this provision on a case-by-case basis, determined by what is deemed to be in the "best interests" of the university.

7.0 Policy Exceptions and Exclusions

- 7.A Seattle Pacific University computer accounts and network resources are intended for use by SPU faculty, staff and students. All users are expected to understand and abide by the provisions set forth in the University's Acceptable Use Policy.
- 7.B Other parties will not generally have access to campus computer resources unless they are granted "exception" status by the appropriate university authority.
- 7.C Seattle Pacific University reserves the right to modify these provisions on a case-by-case basis, determined by what is deemed to be in the "best interests" of the University.
- 7.D Exceptions and exclusions to the policies and procedures outlined herein must be formally approved by the department's Dean or Vice President, and communicated to CIS at least 48 hours in advance of any scheduled automatic or manual processes.