

Computer and Information Systems Policies, Procedures, Plans and Standards

Security: SPU Network Guest Accounts

Effective Date: March 30, 2006

Contents:

1.0 Introduction/Purpose

2.0 Definitions

- A. Guest Account Access
- B. Conference Services Guests
- C. Officially Sponsored Guests
- D. Sponsoring Agent

3.0 Basis for Guest Account Access

- A. Technical Security Requirements Governing Guest Access Policies
- B. Conditions Under Which Guest Account is Permitted
- C. Conditions Under Which Guest Account is Denied/Prohibited
- D. Provisions for Revocation of Guest Account Access

4.0 Provisions for Conference Services Guest Accounts

- A. Conference Services Responsibilities
- B. CIS Responsibilities
- C. Methodology for Guest Account Assignment

5.0 Provisions for Official-Sponsored Guest Accounts

- A. Sponsoring Department Responsibilities
- B. CIS Responsibilities
- C. Methodology for Guest Account Assignment

1.0 Introduction/Purpose

This policy sets forth provisions and responsibilities associated with guest account access to the Seattle Pacific University network. As a protected network, all usage is subject to appropriate use provisions as set forth in the University's Acceptable Use Policy (AUP). SPU's network requires that access and usage be restricted to persons operating in an official capacity at the university. For most people, namely university students, faculty, and staff members, credentials to access the network are automatically generated from within the MARS layer of the Banner Information System. With these credentials, users are free to use the wired and wireless networks at will, within the guidelines of the AUP. Some university affiliates, however, are not in the Banner Information System, and consequently do not have account access by default. This policy provides structure and methodology for assigning guest access to such individuals.

2.0 Definitions

- A. Guest Account Access is defined as access to the university's protected network with credentials other than those generated automatically within the Banner Information System. Such accounts are authorized for use by individuals or groups for a limited period of time. Presently, guest accounts are configured within the Cisco Clean Access System, and are internally referred to as "Local Users."
- B. "Conference services guests" are those persons attending the university in an official capacity as arranged through the Office of Conference Services. As part of a group, these agencies or individuals pay a fee for the use of university resources (housing, classrooms, facilities, networking, etc.). Guest access is provided as a temporary convenience, not as a guaranteed resource, and is subject to the rules and provisions of the AUP.
- C. "Officially sponsored guests" are persons attending the university in an official capacity as arranged through a university department and as part of an officially-sanctioned university event. Such agencies or individuals may or may not pay a fee

for the use of university resources. Guest access is provided as a temporary convenience, not as a guaranteed resource, and is subject to the rules and provisions of the AUP.

- D. "Sponsoring agents" are those individuals or departments of the university that serve as the primary contact point for the guest individual or agency.

3.0 Basis for Guest Account Access

- A. Technical Security Requirements Governing Guest Access Policies
 - There exist three technical security requirements for network access, as defined by Computer and Information Systems and articulated in the AUP:
 - 3.A.1 All persons accessing the SPU network resource must be authorized to do so, as official university students, faculty, staff members, or as official guests of the university.
 - 3.A.2 All devices on the network must be identifiable by a unique MAC address, and associated with an IP address and a user name as noted in item 3.A.1 above.
 - 3.A.3 Each device connecting to the network must be patched and updated, so as to be safe from virus infection or propagation; this provision may be enforced via Group Policy, Cisco Clean Access, or whatever technology CIS has determined to be appropriate.
- B. Conditions Under Which Guest Account is Permitted
 - 3.B.1 Guest account is permitted to university affiliates provided the security policies and provisions in the AUP and policy 3.A of this document are met and approved/coordinated between CIS and the sponsoring university agency.
- C. Conditions Under Which Guest Account is Denied/Prohibited
 - 3.C.1 Guest access is prohibited for all types of access not covered in 3.B.1.
- D. Provisions for Revocation of Guest Account Access
 - 3.D.1 In the event that a device is found to be in violation of the provisions set forth herein, the university reserves the right to revoke network access to the individual, device, or group, depending on the circumstances of the incident, and as determined by the responding CIS staff member.

4.0 Provisions for Conference Services Guest Accounts

- A. Conference Services Responsibilities
 - 4.A.1 Conference Services (CS) serves as the official university agent sponsoring those guests who use campus facilities on a contractual basis. During such times, CS also serves as the official conduit between CIS and the conference guest. CS shall arrange for network access permissions as determined at the time of conference registration, and communicate conference guest access requirements to CIS in a timely fashion. Upon receiving guest account credentials from CIS, CS will assist the conference in basic communication and connectivity issues. CS will collect access fees as appropriate, and authorize the transfer of such funds to CIS via ID entry.
 - 4.A.2 Guest access account requests should include specific dates of the conference, the number of persons attending the conference, and a primary contact number for the conference agent or representative.
 - 4.A.3 Communication about the provisions and circumstances of guest account access as set forth in this document and the AUP is to be communicated to the conference guest by CS in advance of guest account access.
- B. CIS Responsibilities
 - 4.B.1 CIS is responsible for establishing guest access accounts, communicating such information back to CS for guest dissemination, and for terminating guest access after the conference concludes.
 - 4.B.2 CIS reserves the right to immediately and without notice terminate guest account access in the event such access is found to be in violation of the policies set forth herein.
- C. Methodology for Guest Account Assignment
 - 4.C.1 CIS reserves the right to determine appropriate guest account assignment based upon the needs of the university, the department, or the requesting conference. In general, conference guests will be given generic, shared, user account names whenever practical. In some instances, CIS may ask for the specific names of individuals needing guest access and create personalized credentials for each user.

5.0 Provisions for Official-Sponsored Guest Accounts

- A. Sponsoring Department Responsibilities
 - 5.A.1 A sponsoring department serves as the official university agent for guests using campus facilities in performance of activities and responsibilities directly associated with officially-sanctioned and sponsored university-wide events. During such times, the sponsoring department also serves as the official conduit between CIS and the official guest. The sponsoring department shall arrange for network access

permissions and communicate guest access requirements to CIS in a timely fashion. Upon receiving account credentials, the sponsoring department will assist the guest in basic communication and connectivity issues.

5.A.2 Communication about the provisions and circumstances of guest account access as set forth in this document and the AUP is to be communicated to the official guest by the sponsoring agency in advance of guest account access.

B. CIS Responsibilities

5.B.1 CIS is responsible for establishing guest access accounts, communicating such information back to CS for guest dissemination, and for terminating guest access after the period for authorized access.

5.B.2 CIS reserves the right to immediately and without notice terminate guest account access in the event such access is found to be in violation of the policies set forth herein.

C. Methodology for Guest Account Assignment

5.C.1 CIS reserves the right to determine appropriate guest account assignment based upon the needs of the university, the department, or the requesting user or agent. In general, official guests will be given generic, shared, user account names whenever practical. In some instances, CIS may ask for the specific names of individuals needing guest access and create personalized credentials for each user.