

Seattle Pacific University

Computer and Information Systems

Policies, Procedures, Plans and Standards

Privileged Account Audit and Use Policy

Effective: December 9, 2006
Updated and Approved by CIS: February 2, 2009

Contents:

1.0 Introduction/Purpose

2.0 Definitions

- A. Granting Agent/Authority
- B. Types of Resources/Accounts
- C. Levels of Access
 - 2.C.1 Operational Access and Resource Management
 - 2.C.2 Inquiry/Investigation
 - 2.C.3 Review/Interrogation
 - 2.C.4 Modification/Removal
 - 2.C.5 Analysis and Interpretation
 - 2.C.6 Never Ask for Passwords From the User

3.0 Privileged Access Requirements

- A. Requirement for Written Authorization
- B. Criteria for Legitimacy

4.0 Investigative Process and Auditing

- A. Prior Approval
 - B. Authorized and Unauthorized Activities
 - C. Requirement for Audit Recording
 - D. Requirement for Notification
 - E. Exclusions from Notification Requirement
 - F. Modification/Removal Requirements
-

1.0 Introduction/Purpose

As part of network and server management responsibilities, certain staff members in CIS have heightened administrative computer account privileges. These accounts (hereafter "SysAdmin") have considerable authority to access, manage and even take-over those accounts used by students, faculty and staff members of SPU. This policy sets forth the guidelines and principles for CIS staff use of SysAdmin privileges, specifically as these rights are associated with general resource accounts.

2.0 Definitions

- A. Granting Agent/Authority
CIS staff members do not normally access privileged or private account information or content in the performance of their core responsibilities and duties. SysAdmin access or audit activities, as they relate to individual/personal accounts of the general user community, are usually performed at the request of the individual owner of the account/resource or under the direction of a person with executive management authority within the University. For purposes of definition, this executive authority must come from the Assistant Vice President for Technology Services, a Vice President, or the President. A person acting as the "designate" for the authority may also provide approval or direction.
- B. Types of Resources/Accounts
It is recognized and understood that all user accounts, system resources, server applications, and data stored, belong to the University in the context that these resources are hosted or maintained on campus owned property for legitimate institutional or educational purposes. It is also recognized and understood resources such as user accounts, domain accounts, email accounts and network file space are allocated to individual faculty, staff or students for their personal use under the guidelines of the SPU Acceptable Use Policy. CIS will recognize the "named resource owner" as the primary user of the computer account or resource.
- C. Levels of Access
 - 2.C.1 Operational Access and Resource Management
Activities that are performed in the regular and operational maintenance of accounts and resources. Tasks such as password and credential resets, moving resources between systems and resources, regular data backups and restores, quota management, network access permissions and policies; are examples of operational maintenance.
 - 2.C.2 Resource Inquiry
Activities that involve reviewing account details to determine if resources are present or if data are accessible are considered actions of resource "inquiry." Actions of inquiry focus on the presence and availability of a resource, and typically do not involve the potential disclosure of confidential or special personal information.
 - 2.C.3 Investigation/Interrogation

Activities that involve the specific analysis, investigation or interrogation of the actual contents of a computer or network resource are labeled as “investigation.” Information gathered as part of this level of investigation hold the potential to expose confidential or special personal information. Data collected under this level of access may be provided to the appropriate campus or external authority for further review and action.

2.C.4 Modification/Removal

Activities that modify or remove *content* from a computer or network resource require significant review and the highest level of approval and authorization. There must be an “significant ramification” for this type of activity. Documentation and sufficient record keeping is essential for this level of access.

2.C.5 Analysis and Interpretation

SysAdmin activities shall be limited to obtaining and providing data to the University’s granting authority or designee. It is not the responsibility of the CIS staff member charged with resource inquiry or investigation to analyze the content of such information in order to interpret or rule on aspects of legality or impropriety.

2.C.6 Never ask for passwords from the User

Due to the increased frequency of phishing email scams and other social engineering techniques to compromise account credentials, CIS SysAdmin staff are encouraged to never ask a user for their account password. The only exception to this rule is in the case where trouble shooting or correcting a specific credential problem must use the existing password. In this case the account holder will be required to change the password once the problem has been resolved.

3.0 Privileged Access Requirements

A. Requirement for Written Authorization

CIS staff members are authorized to act as agents on behalf of the University in instances where privileged account access or related audit activity is not approved by the resource owner, but under the direction of a person with executive management authority within the University as pursuant to item 2A, above. All such CIS activities shall require written authorization in advance of SysAdmin privileged access use. Such written authorizations will include details regarding:

- 3.A.1 the granting SPU authority;
- 3.A.2 the identify of the resource(s) under review;
- 3.A.3 a description of the specific activities to be performed by the CIS staff member;
- 3.A.4 instructions outlining the specific methods in which evidence is to be preserved and data are to be handled (sealed; archived; copied; confiscated; etc.)
- 3.A.5 the timeframe for which the inquiry is authorized; and
- 3.A.6 requirements and methods for forwarding/providing data to the University’s investigative designee.

B. Criteria for Legitimacy

Because the use of privileged account access tools in the context of investigative activity may intrude upon the privacy of individually held resources, there exists a high burden of proof to justify the use of such powers without a prior consent on the part of the individual under investigation/audit. The intent here is not to list specific criteria that **MUST** be met in order for such a burden of proof to be met. Rather, the criteria listed below are to serve as examples of the things that should (and should not) be legitimate reasons for privileged account access to individual user credentials:

- 3.B.1 Investigation into confirmed or suspected breaches in violation of Federal or Statutory requirements (FERPA, HIPAA, SPI Breach, etc.)
- 3.B.2 Investigation into areas of imminent health and safety.
- 3.B.3 Investigation involving a confirmed or suspected attempt to compromise server or network resources.
- 3.B.4 Investigation involving a confirmed or suspected violation of the University’s Acceptable Use, employment, or student lifestyle expectations policies.
- 3.B.5 Investigations that are lead by an official police or legal authority under the direction of University Counsel or other campus representatives.
- 3.B.6 Collection of stored information in log files, computers, or network resources for the purpose of preserving a known state for later review.
- 3.B.7 Removal of illegal data or material under the direction of the appropriate campus or external authority.

4.0 Investigative Process and Auditing

A. Prior Approval

Activities that require SysAdmin evaluated access that are approved in advance by the resource owner are considered routine and do not require additional review or approval. Care should be taken to verify access and confirm actions taken with the resource owner when performing these tasks.

B. Authorized and Unauthorized Activities

Activities for privileged access are to be outlined in writing as prescribed under 3A. Under no circumstances will privileged access be done in a manner that is untraceable and not subject to audit. All SysAdmin investigative activities shall be done using a SysAdmin account; audit activities will not generally be done in a manner by which the investigative authority ‘assumes’ the identity of the person under investigation.

C. Requirement for Audit Recording

All activities done in the context of the investigation shall be documented. This documentation should include the date and time activities occurred; the actions taken; the name and title of the person conducting the audit; and a list of witnesses or reviews of the investigative activity. This audit recording shall become part of the official, written investigative transcript begun with the written authorization detailed under 3A.

D. Requirement for Notification

Following the investigation or resolution, the person/resource under audit should generally be notified that the privileged access to their account was conducted, and if requested --provided a transcript of the audit activity as outlined in 3A and 5B. Exceptions to this notification step are outlined below.

E. Exclusions from Notification Requirement

In the event that audit activities are being conducted on the basis of confirmed or suspected criminal activity, confirmed or suspected campus policy violation, or confirmed or suspected system compromise; the requirement for notification as set forth in 5C may be waived provided that

this exclusion is made in writing on behalf of the investigative authority and/or University Counsel, and that such documentation become part of the official investigative record.

F. Modification/Removal Requirements

If the activity requires the modification or removal of any data or information, the original data or material should be preserved in such a manner that subsequent review or audits could be performed. This may include providing the original information in the investigative record.

End of Document