Privileged System Access Policy

Statement and Purpose

Seattle Pacific University possesses exclusive rights over the information within its systems. This includes business plans, academic records, financial information or other sensitive materials and information in printed, electronic or signed/spoken form that may affect employee rights or the organization’s operations.

This policy sets forth expectations and responsibilities associated with being granted privileged access to university systems and data. Privileged users assume additional responsibility for ensuring the integrity, confidentiality, and availability of the data and resources they manage by nature of their roles.

Persons in these positions are given broader access to computer systems and resources because their job responsibilities require such access. Roles requiring privileged access are granted significant trust and expected to use their privileges appropriately for their intended purpose, and only when necessary to maintain systems and data they steward. Any private information seen in carrying out these duties must be treated in the strictest confidence. If a privileged user violates the terms of this policy, the privileged user and/or the University may be exposed to liability.

At all times the use of technology resources falls within the University’s Computer Acceptable Use policy.

There are many types of Computer User Accounts and Resources that are made available to SPU faculty, staff, students, and even former students. This policy includes all SPU provided or managed accounts and resources – whether hosted on-site or in the cloud.

Certain terms in this policy are defined at the end of the policy.

- Download Policy as PDF
- Download Signature Page
- Signature Page Library

Privileged Access

Privileged access, commonly referred to as supervisor, system administrator, admin, or root access, grants an individual non-standard elevated access to the resources and data to perform system/data administration job duties. University staff with privileges or access used to administrate systems or data is considered a user with privileged access.

Requirements for Privileged Access

- Privileged access is only be granted to employees requiring elevated access to perform documented job responsibilities.
- CIS may require an in person meeting and/or technical skills assessment to demonstrate competency prior to granting privileged access.
- Eligible employees are required to sign and agree that they have read, understand, and will comply with the policy prior to being granted privileged access. Signed agreements will be kept on file by the CIO in the department of Computer and Information Systems.

⚠️ Administrative credentials are not to be shared or disclosed under any circumstance, except with the express approval of the CIO.

Agreements by Privileged Users:

Privileged users agree to use privileged access appropriately, respect privacy, protect institutional data, and enforce security and legal compliance, as more fully described below.

Use Privileged Access Appropriately

1. Administrative credentials are not to be used as a primary login for non-privileged access and activities.
2. Privileged access may only be used when performing administrative job duties that require elevated permissions.

Respect Privacy
Privileged users should never “browse” through the another persons personal data or institutional data while using privileged access, unless such browsing is a specific part of their job description (e.g. computer auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior; or is specifically requested by, or has the approval of, the person who authorized the privileged access.

a. Investigative activities must be authorized by the SPU president, provost, VP or the CIO. See CIS Privileged Account Usage for details.

2. Privileged users should protect the confidentiality of any information they encounter while performing their duties. Unauthorized disclosure of confidential information could seriously and adversely impact SPU, its students, and other individuals and organizations associated with SPU.

3. Privileged users should never disclose to any unauthorized person any institutional data observed while operating with privileged access.

4. Privileged users should not copy any institutional data observed while operating with privileged access for any purpose other than those authorized under their defined job responsibilities.

Protect Institutional Data

1. Privileged users should seek to protect institutional data and should not intentionally or recklessly damage or destroy any Institutional Data. See Institutional Data Policy for details.

2. Privileged users should not take actions on computer systems under their charge that will impair the integrity or security of that system or other University systems.

3. Privileged users should not modify or delete institutional data unless it is done in accordance with SPU policies and procedures.

Enforce Security and Legal Compliance

1. Privileged users should use all available protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.

2. Privileged users should report all suspicious requests, incidents, and situations regarding an SPU computing resource to an appropriate member of management or the CIO.

3. Privileged users should comply with all computer security standards and policies in force at SPU.

4. Privileged users should not attempt to gain or use privileged access outside of assigned responsibilities, or beyond the time when such access is no longer required in job functions.

5. Privileged users should not tell or disclose to any unauthorized person the information required to gain privileged access, and should not engage in careless practices that would reveal that information to unauthorized persons.

6. Privileged users should not change or develop any computer software in such a way that would (1) disclose computer information to unauthorized persons or (2) make it possible to retain any special access privilege, once that authorized privilege has been terminated by management.

7. Privileged users should not do special favors for any user, member of management, friend, or any other person regarding access to SPU computing resources that would circumvent prevailing security protections or standards or would otherwise violate this policy.

8. Privileged users should maintain awareness and responsibility for complying with all applicable laws, regulations, policies, and procedures.

Granting of Permissions

Many privileged users have the ability to grant access to SPU systems and/or institutional data they administer, including the ability to grant others privileged user access to that system. Privileged users are responsible for permissions they grant as follows:

1. Privileged users who authorized the

2. Privileged users must ensure that

3. Privileged users must not

When granting permissions, privileged users are responsible for:

1. Following any policy or procedure governing the granting of permissions or access related to the system in question.

2. Receiving authorization from a system owner, supervisor, or other administrator authorizing the granting of permissions.

3. Questioning the requester and/or approver to ensure appropriate access is being granted.

When granting privileged access, privileged users are responsible for:

1. Following all the above noted responsibilities for granting permissions.

2. Referring new privileged users to training materials, documentation, and/or policy relevant to their new access.

3. Obtaining a copy of this policy, signed by the requester, (i.e., the individual requesting privileged access), the department approver, and the approving department head or director.

4. Following a least privileges methodology, granting only access required by the grantee's job duties and nothing more.

When granting permissions, approvers are responsible for:

1. Following any policy or procedure governing the granting of permissions or access related to the system in question.

2. Verifying with the grantor that the access/permissions are appropriate for the requester.

Revocation of Privileged Access
Privileged users must always be aware that these privileges place them in a position of considerable trust. Privileged users must not breach that trust by misusing privileges or failing to maintain a high professional standard.

Definition of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>The ability to view, use, or change information in University databases, systems, or other computer resources.</td>
</tr>
<tr>
<td>Confidential Information</td>
<td>Information that is very sensitive in nature and is, in some cases, protected by laws and statutes. These require careful controls and protection. Examples include: personally identifiable information, protected health information, employment records, student records, financial records, social security numbers, credit card numbers, legally protected University records, and passwords.</td>
</tr>
<tr>
<td>CIO</td>
<td>The University’s Chief Information Officer (i.e., the Assistant Vice President for Technology Services).</td>
</tr>
<tr>
<td>Institutional Data</td>
<td>Any and all data that is collected and maintained by Seattle Pacific University related any university operations.</td>
</tr>
<tr>
<td>Disclose</td>
<td>Make known, reveal, release, transfer, or provide access to any institutional data in any manner.</td>
</tr>
</tbody>
</table>
| Personally Identifiable Information (PII) | Personally Identifiable Information (PII) is information that is a subset of individual and student information, including demographic, financial, or sensitive information collected from an individual and:  
  • That identifies the individual; or  
  • With respect to which there is a reasonable basis to believe the information can be used to identify the individual. |
| Privileged Access                | Access that allows the grantee non-standard or elevated privileges allowing access to administrate systems or data. This includes the ability to alter system configurations, manage software systems, grant access, etc. It also includes elevated access to Institutional Data enabling direct SQL querying, data management, data maintenance, or reporting. |
| Privileged User                  | Any individual granted privileged access to information, systems, or databases at at Seattle Pacific University that extends beyond access to one’s own self-service data. |
| Protected Health Information (PHI) | Protected health information means individually identifiable health information that is protected by HIPPA.                              |
| Safeguard                        | Protect or cover from exposure, using precautionary measures.                                                                            |
| System Administrator             | System administration duties consist of all aspects of managing a technology-based information system, including but not limited to, user administration, front-office and back-office hardware and software configuration and management, data base administration, and network, domain, and other technology infrastructure management. |

SPU Related Policies and Procedures:

Invalid License
License is not configured.