SLAC NATIONAL ACCELERATOR LABORATORY

Acceptable Use of Information Technology Resources Policy

Document Approval (signature/date)

Chief Information Officer:	Theresa Bamrick	5/3/19	Theresa Bamrick

Table of Contents

1.0 PURPOSE

This policy establishes and outlines the acceptable use of SLAC information technology (IT) resources and ensures that controls are in place to maintain the confidentiality, integrity, and availability of information processing and communication services on systems managed by SLAC.

2.0 AUTHORITY AND APPLICABILITY

2.1. Authority

This document is issued under the authority of the Laboratory Director to direct the management and operation of the Laboratory. The authority to implement the program requirements has been delegated by the Director to the Chief Information Officer.

This document identifies specific requirements, roles, and responsibilities for the Laboratory Director, Managers, SLAC personnel, users, and the Computing Division.

2.2. Applicability

This document applies to all employees and users of SLAC information technology. SLAC information technology resources include all hardware, software, networks, electronic mail (e-mail), as well as all SLAC data.

3.0 PROGRAM DESCRIPTION

SLAC information technology resources are government assets for SLAC-related business use. Unauthorized use is prohibited. Inappropriate use exposes SLAC to risks including malware, compromise of network systems and services, and legal issues. Minor incidental personal use is permitted. SLAC reserves the right to audit networks and systems using SLAC information technology resources on a periodic basis to ensure compliance with this policy. See Limited Personal Use of Government Office Equipment including Information Technology and the Stanford Administrative Guide.

3.1. Acceptable Use of IT Resources

- Individual SLAC computer accounts are intended for use only by the user assigned to that account. Each account holder is responsible for the resources used by that account and for taking necessary precautions to prevent others from using the account.
- Shared accounts require adequate justification and explicit authorization from the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO).
- Passwords must be chosen with care and not divulged to anyone under any circumstances. Different classes of systems, for example business systems, scientific computing systems, and accelerator control systems may have different requirements for user passwords. Users are responsible for following the password policies for the systems

on which they have accounts. Your password should not be disclosed to anyone under any circumstances, including when requested by anyone claiming authority to do so.

- Before leaving a system unattended, it must be adequately protected, e.g. by locking the screen or logging off the system.
- Users must safeguard legally protected information subject to privacy laws or confidentiality requirements.
- All SLAC and Stanford policies apply to use of SLAC information technology resources especially, but not exclusively, policies on intellectual property, misuse of resources, harassment, and information and data security.
- Systems accessing the secure network must be centrally managed, unless an approved exception request is granted by the CIO or CISO.

3.2. Misuse of IT Resources

Users have an affirmative duty to report suspected misuse of SLAC information technology resources immediately to the Computing Division help line (x4357) or the SLAC CISO. Misuse of SLAC information technology resources includes, but is not limited to:

- Engaging in any activity that is illegal under local, state, federal or international law while utilizing SLAC owned resources.
- Using SLAC's electronic communication facilities to send fraudulent, harassing, offensive, threatening, inappropriate, or sexual content. Stanford’s University Code of Conduct applies.
- Seeking to gain or enable unauthorized access to information technology resources.
- Using SLAC information technology resources to support running a business, paid consulting, or lobbying of any kind.
- Impacting or interfering with the work of another employee or correct functioning of any SLAC information technology resource.
- Cryptocurrency mining activities are explicitly prohibited.
- Unauthorized use of copyrighted material including, but not limited to, downloads of copyrighted material, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SLAC or the end user does not have an active license.
- Circumventing security controls.

3.3. Violation of Policy

Any SLAC employee found to have intentionally violated this policy shall be subject to disciplinary action up to and including termination. A user violating this policy may have

their computer removed from the network, and any SLAC network or computer access disabled. Reinstatement will require the review and approval of the Chief Information Officer (CIO) with concurrence from the CISO and appropriate Associate Laboratory Director. Equipment may be confiscated for forensic review with concurrence or direction from Legal and/or Human Resources.

3.4. Exceptions to Policy

Any exception to this policy must be in writing and approved by the CISO with concurrence from the CIO.

4.0 RESPONSIBILITIES

This document defines specific roles, responsibilities, and requirements for implementing the acceptable use of information technology resources program.

4.1. Laboratory Director

- Sets policy and expectations and provides the institutional authority for the acceptable use of information technology resources program.

4.2. Senior Management Team

- Ensures that management, supervisors, and staff are aware of, and adhere to, the approval and delegation authority requirements in this document.

4.3. Chief Information Officer

- Has overall responsibility for acceptable use of information technology resources.
- Maintains this policy document.

4.4. SLAC Personnel and Users

- Responsible for the acceptable use of information technology resources.
- Protect business and scientific data, and personally identifiable information (PII).

4.5. Computing Division

- Protects information and resources from unauthorized use.
- Defines and implements acceptable use for information technology resources guidelines.

5.0 IMPLEMENTATION

This document is effective on the date of issue.

6.0 TRAINING

No training is required for implementing this policy.

7.0 DOCUMENTS AND RECORDS

The SLAC Institutional Policies site (https://policies.slac.stanford.edu) will contain the official record for this document.

8.0 DEFINITIONS AND ACRONYMS

Users – All those who have access to SLAC information technology resources.

9.0 REVISION HISTORY

Revision	Date Released	Description of Change
R001	5/12/2014	New Document
R001.1	8/12/2015	Annual Review. Grammar and changes for clarification. System Security Plan information.
R002	5/3/2019	Transition to new IRP template and updates to include authority and applicability descriptions as well as misuse guidelines.

10.0 REFERENCES

- Minimum IT Equipment Security Requirements
- ServiceNow Service Catalog
- Code of Federal Regulations 5 C.F.R. § 2635.704 through .705: Use of Government Property and Use of Official Time
- Limited Personal Use of Government Office Equipment including Information Technology
- Stanford Administrative Guide
- Stanford University Code of Conduct