SLAC NATIONAL ACCELERATOR LABORATORY

Acceptable Use of Information Technology Resources Policy

Document Approval (signature/date)

Chief Information Officer:	Jonathan Russell Jonathan Russell (Feb 7, 2024 17:42 PST)	Feb 7, 2024	Jonathan Russell

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 SLAC IT.

2.2. Applicability

This document applies to all employees and users of SLAC information technology. SLAC information technology resources include all hardware, software, networks, and cloud services, as well as all SLAC information.

3.0 PROGRAM DESCRIPTION

SLAC adheres to the Stanford Administrative Guide 6.2.1 Computer and Network Usage policy, with additional requirements to support DOE and federal compliance. SLAC information technology resources are government assets for SLAC-related business use. Unauthorized use is prohibited. 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 the Stanford Administrative Guide and Limited Personal Use of Government Office Equipment including Information Technology.

3.1. Acceptable Use of IT Resources[1]

- SLAC prohibits the use of Personally Owned Computers to connect to any SLAC owned or managed network, or for work and/or research purposes except through authorized service gateways or specifically approved applications.

  "Personally Owned Computers" are information resources that are under the control of SLAC employees or agents and are not wholly owned and managed by SLAC.

[1] Additional guidance on the Incidental Use of Personally Owned Computers is provided at https://slacprod.servicenowservices.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D42a6b9dc8710c214753a21f5cebb356d%26preview_article%3Dtrue

- The following activities must ALWAYS be conducted using a SLAC owned and managed device:
    - Budget
    - Sensitive Data (e.g., SPI)
    - Finance
    - Official Correspondence with DoE
    - Supervisory duties (e.g., performance reviews)
- Personal mobile devices are permitted to be used for work and/or research if the device is registered with SLAC IT and work applications and data are isolated and managed by SLAC approved tools.
- Use of an email client on a personal mobile device to directly access SLAC email/ calendar is permitted only if the device is SLAC registered and managed..
- Collaborative researchers, visiting faculty and non-primarily Stanford employees working at SLAC may use their institution-issued systems for work and/or research at SLAC through approved service gateways.
- SLAC resources are to be used for SLAC work and/or research purposes only. Incidental use for personal or emergency reasons is permitted but must not interfere with or violate SLAC policies or protections.
- Systems accessing the SLAC network must be managed with SLAC configuration software unless an exception request is approved by the CIO or CISO.
- 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 are strongly discouraged and are being phased out; use service accounts instead when appropriate. Shared accounts required for mission support must be approved annually by 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 password requirements. 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 the use of SLAC information technology resources especially, but not exclusively, policies on intellectual property, misuse of resources, harassment, and information and data security.
- Having or using the TikTok social networking service (or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited) is prohibited on information technology used in the performance of the SLAC/DOE contract (or subcontract at any tier) if the equipment is:
    - owned or managed by the U.S. Government

      OR

    - used or provided by SLAC, a SLAC employee (including employee-owned devices), or a SLAC subcontractor in the performance of the SLAC/DOE contract (or subcontract), when the SLAC/DOE contract (or subcontract) requires use of the equipment or requires use to a significant extent in the performance of a service or the furnishing of a product.

  These prohibitions do not apply to any equipment acquired or used incidental to the SLAC/DOE contract (or subcontract).

3.2 Acceptable Use of Artificial Intelligence Tools

- Employees have the responsibility to ensure all use of Artificial Intelligence in support of research is consistent with the Stanford Research Policy Handbook.
- If Generative Artificial intelligence (GenAI) tools are used in a research context, clearly cite their usage, and describe them as part of the research methodology.
- The use of GenAI or Large Language Model (LLM) software at SLAC is governed by the same rules as all other third-party software tools.
- Employees must use GenAI in a manner that aligns with SLAC's mission and values.
- Employees must not disclose data owned by SLAC or that SLAC has a responsibility to protect (confidential or proprietary information) to a GenAI technology, directly or through a third party application, without specific approval for the tool.

  This data includes, but is not limited to, Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), Official Use Only (OUO) information and Export-Controlled Information.
- Output of GenAI tools may be subject to third party copyright and must not be included directly into any SLAC owned or managed tools, code, or work product unless robust

measures have been taken to ensure the learning datasets are not legally restricted by copyright or similar.

- Any usage of GenAI tools must not presume correctness or coherence for any results produced. LLMs are designed to provide responses that are verbose but could be limited, biased, out of date, or incorrect. Verify any responses produced.

3.3. Misuse of IT Resources

- Users have an affirmative duty to report suspected misuse of SLAC information technology resources immediately to SLAC IT Services 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.
- Use of SLAC information technology resources to mine cryptocurrency is strictly prohibited.
- Impacting or interfering with the work of another employee or correct functioning of any SLAC information technology resource.
- Unauthorized use of copyrighted material including, but not limited to downloading or distributing copyrighted materials, including textual, audio, and video materials, without the consent of the owner of the copyright.
- Installation or use of any software for which SLAC or the end user does not have an active license.
- Circumventing or attempting to circumvent security controls.

3.4. 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.

3.5. 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 (CIO)

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

4.4. Chief Information Security Officer (CISO)

- With CIO, approves exceptions to this policy.
- Handles reports of suspected misuse of information technology resources.

4.5. SLAC Personnel and Users

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

4.6. SLAC IT

- 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.
R003	10/20/2022	Changes based on review.
R004	2/7/2024	Addition of Acceptable Use of Generative AI Tools section, revisions related to TikTok, and the use of Personally Owned Computers.

10.0 REFERENCES

- Guidance on Use of Personally Owned Computers
- 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
- Stanford Research Policy handbook
- Responsible AI at Stanford