# San Diego Supercomputer Center (SDSC)
# Triton Shared Computing Cluster
# (TSCC COMPLIANCE SYSTEM)
# CUI (Controlled Unclassified Information)/CAD (Controlled Access Data) / NIST 800-171
# Acceptable Use Policy (AUP)

---

Version 1.1

This document contains the full TSCC COMPLIANCE SYSTEM CUI (Controlled Unclassified Information)/CAD (Controlled Access Data) Acceptable Use Policy and the User Agreement & Sign-Off Form.

# TSCC COMPLIANCE Acceptable Use Policy for CUI/CAD / NIST 800-171–Compliant Operations

## 1. Purpose

This Acceptable Use Policy (AUP) defines the responsibilities and required behaviors for all users of the San Diego Supercomputer Center's (SDSC) Triton Shared Computing Cluster (TSCC Compliance) resources designated for processing, storing, or transmitting Controlled Unclassified Information (CUI/CAD) in compliance with NIST SP 800-171. This AUP applies only to in-scope TSCC COMPLIANCE resources:

- TSCC Compliance login nodes
- TSCC Compliance compute nodes (batch scheduled)
- USS storage systems designated for CUI/CAD
- Internal authentication, authorization, job scheduling, and management systems that support TSCC Compliance CUI/CAD operations

---

## 2. Authorized Use and Users

Client workstations are designated as non-CUI systems and are not a part of the authorized system boundary for CUI/CAD processing. Users shall not copy, download, upload, synchronize, screen capture, or otherwise transfer CUI/CAD from authorized systems to client workstations. CUI/CAD must remain contained within the TSCC Compliance System at all times. Further data handling and storage restrictions are detailed below. Exporting decontrolled CUI is allowed via approved transfer mechanisms as documented in the TSCC Compliance Plan.

Access to TSCC Compliance System CUI/CAD-compliant resources is restricted to:

- Approved researchers, staff, and project personnel associated with a CUI/CAD authorized allocation
- Users explicitly sponsored by a Principal Investigator (PI) or Project Point of Contact (POC)
- Individuals who have completed all required training and obtained Duo MFA credentials for SDSC systems

Use of TSCC Compliance systems is limited to activities directly related to approved research or project work involving CUI/CAD or other permitted datasets.

Use for personal, recreational, or unrelated commercial purposes is prohibited.

---

## 3. External Researcher/User

An *External Researcher/User* is defined as a standard, non-privileged user of the TSCC Compliance System who is not affiliated as a UC San Diego faculty member, staff, or student. Once granted access, external users are subject to the same in-system controls and restrictions as internal users as outlined in this document, in addition to the requirements below.

**Additional Requirements for External Researchers:**

- The Principal Investigator (PI) or sponsoring organization ("Parent Organization") is solely responsible for ensuring that all external users are properly authorized prior to access. This includes verifying that each user has obtained all required approvals, attestations, and permissions necessary to access, download, or use Controlled Unclassified Information (CUI) or other restricted datasets in accordance with NIST SP 800-171.
- The PI or parent organization is solely responsible for conducting any required background checks, user vetting, user training, and eligibility determinations for its personnel and authorized users.
- The PI or parent organization is solely responsible for ensuring compliance with all applicable data use agreements, regulatory requirements, and legal obligations associated with its datasets and research activities.
- The PI or parent organization is solely responsible for managing the compliance of the endpoints used by their employees to access the TSCC Compliance system.
- The PI or parent organization is solely responsible for securing and protecting any CUI data that is removed from the TSCC Compliance System.
- The PI, Parent Organization and External Researcher must ensure that any suspected or confirmed security incidents, unauthorized access, or data breaches involving TSCC resources or data are promptly reported to SDSC/UC San Diego in accordance with institutional incident reporting requirements.
- By requesting or maintaining access, the PI, Parent Organization and External Researchers explicitly acknowledge and accept full responsibility for the compliance posture of their users and environments, and any risks arising from their access to TSCC systems.

---

## 4. Account Credentials and Authentication

1. Each user will receive one TSCC Compliance System account and must protect their passwords, SSH keys, and Duo MFA credentials.
2. Users must not share accounts, credentials, SSH keys, or Duo authentication methods with any other person.
3. All access to TSCC Compliance CUI/CAD systems must occur via SSH with Duo Multi-Factor Authentication**.**
4. Access from mobile devices is prohibited.
5. Accounts may be suspended or revoked if misuse, compromise, or unauthorized access is suspected.
6. Sessions will automatically terminate after 90 minutes of inactivity.

---

## 5. System Access and Restrictions

1. Users may access the TSCC Compliance environment only through approved TSCC Compliance System Login nodes.
2. TSCC Compliance and USS System Users and Staff are responsible for safe-guarding CUI/CAD at alternate work sites (i.e., remote access).
3. Direct login to USS storage systems is prohibited; users access storage exclusively via TSCC Compliance login nodes.
4. Compute nodes may be accessed only through the batch scheduler**.** Interactive logins outside scheduler mechanisms are not permitted.
5. Users must not attempt to circumvent access controls, escalate privileges, or probe system security.

---

## 6. Data Handling and Storage Requirements

1. Users may store and process only authorized CUI/CAD and project-approved datasets on TSCC Compliance CUI/CAD systems.
2. CUI/CAD must reside exclusively in approved TSCC Compliance storage locations (USS compliance storage or storage approved by TSCC Administrators).
3. Users may not relocate CUI/CAD to unauthorized storage locations, temporary scratch that is not CUI/CAD-approved, or systems outside the TSCC Compliance System boundary.
4. SDSC Staff shall configure their SDSC endpoints to lock the screen after 60 minutes activity with a pattern-hiding display and recommends that users similarly configure their endpoints.
5. Uploading, transferring, or caching CUI/CAD onto any unauthorized system or device—whether owned by the user or a third party—is prohibited.

6. The TSCC compliance system does not allow the use of external USB devices, removable/portable media, and unapproved external storage to transfer data into or out of TSCC Compliance CUI/CAD systems.
7. If user makes use of a portable storage device on their endpoint, which is out of scope from the TSCC Compliance System, they are responsible for encrypting the device using FIPS 140-2 validated ciphers. If an unencrypted device must be used, or an encrypted device is used, the user is responsible for physically storing the devices in a secure location, maintaining chain of custody control of the device, keeping logs of access, and sanitizing the device after use.
8. The TSCC Compliance system will provide no printing capabilities. If a user prints within their environment, outside of the TSCC Compliance System, they are responsible for protecting and managing any printers or printed material. 9. Users and TSCC Staff shall not connect any removable media to the TSCC Compliance and USS Systems when the owner cannot be identified, or the media lacks proper CUI/CAD markings.
10. The TSCC Compliance system shall not provide backup/archive services to users. If a user/project implements backup/archive of their CUI/CAD data, they are responsible for protecting the data to CUI/CAD requirements including meeting the requirements stated in this AUP.
11. Users are responsible for managing and configuring their endpoints so that they do not create a network bridge between the TSCC Compliance system and other network locations (i.e., no split-tunneling).
12. Users shall not store ITAR, EAR, FISMA, HIPAA, patient personal data or other compliance or export controlled data on the TSCC Compliance System other than CUI/CAD.

---

## 7. Network and Internet Use

1. TSCC Compliance login nodes have outbound internet access for research-related activities such as:
    - Accessing software repositories (e.g., GitHub) ○ Connecting to license servers
    - Obtaining large datasets from approved public sources
2. No web browsers are installed, and users must not attempt to install or run browsers or perform interactive web browsing.
3. The TSCC Compliance system shall not be used to post any public facing CAD or web content.
4. Users must not create unauthorized tunnels, proxies, port forwards, or network services.
5. Peer-to-peer file sharing services (e.g., BitTorrent) are strictly prohibited.
6. While connected to the TSCC Compliance System, users and TSCC Staff must lock or terminate their software applications when leaving their endpoints unattended.

7. Users shall not connect collaborative computing devices to their endpoints while connected to the TSCC Compliance system.
8. Staff and Users are responsible for only connecting to known external safe web-sites and systems.

---

## 8. Software Use and Installation

1. Users may install or compile software only within their home or project directories.
2. Users may not install system-level software, modify operating system components, or run daemons or background services.
3. All installed software must comply with applicable licensing terms, export controls, and sponsor-defined restrictions.
4. Users are responsible for updating and maintaining (i.e., patching) any software that they install within their Home or Project Directories.
5. Software that introduces security risks—such as network scanners, packet sniffers, or exploitation tools—is prohibited unless explicitly authorized for the project.

---

## 9. Responsibility for Computing Behavior

Users must:

1. Operate within resource limits defined by the batch scheduler.
2. Submit jobs that behave cooperatively and do not degrade overall system performance.
3. Avoid running unauthorized long-lived processes on login nodes.
4. Follow PI/POC direction concerning project data, collaboration, and resource allocation.

---

## 10. Expected Conduct and Prohibited Activities

The following actions are prohibited on TSCC Compliance CUI/CAD systems:

- Sharing accounts or logins
- Attempting unauthorized access to the accounts, data, or files of other users
- Attempting to bypass, disable, or interfere with security controls
- Running cryptocurrency miners or other unauthorized compute-intensive workloads
- Installing or using web browsers or interacting with non-research websites

- Using mobile devices to access TSCC Compliance system; Use of mobile devices is limited to MFA only.
- Storing CUI/CAD on mobile devices and mobile computing platforms
- Conducting penetration testing, scanning, or other security attacks
- Storing or processing data in violation of CUI/CAD authorization or sponsor restrictions

---

## 11. Monitoring and Privacy

1. TSCC Compliance CUI/CAD systems are subject to monitoring, logging, and auditing for security, Compliance, and operational needs.
2. Users should have no expectation of privacy regarding activity conducted on TSCC Compliance CUI/CAD systems.
3. Monitoring applies only to in-scope TSCC Compliance systems and does not extend to user endpoints.

---

## 12. Incident Reporting

Users must **immediately report**:

- Suspected account compromise
- Unauthorized access to CUI/CAD
- Loss or corruption of CUI/CAD
- Misuse of TSCC Compliance resources
- Any activity that may pose a security risk

Reports should be made via the TSCC ticketing system (tscc-support@ucsd.edu) or to the designated TSCC Compliance security contacts.

---

## 13. Enforcement

Violations of this AUP may result in:

- Immediate suspension of TSCC Compliance access
- Notification of the PI/POC and sponsoring organization
- Requirement for retraining
- Permanent revocation of TSCC Compliance access
- Institutional disciplinary actions or legal consequences where applicable

SDSC reserves the right to regulate, suspend, or terminate access to TSCC Compliance resources at its discretion to maintain the security and integrity of CUI/CAD systems.

---

## 14. Acceptance

By using TSCC Compliance CUI/CAD-compliant systems, the user acknowledges:

- They have read and understood this Acceptable Use Policy
- They agree to comply with all rules and requirements herein
- They understand that failure to comply may result in loss of access or further action

## Appendix A: Definitions

CUI=Controlled Unclassified Information per NIST 800-171

CAD=Controlled Access Data per the NIH definition

# TSCC COMPLIANCE CUI/CAD System User Agreement & Sign-Off Form

By signing below, I acknowledge that I have read, understand, and agree to comply with the TSCC Compliance Acceptable Use Policy (AUP) for CUI/CAD/NIST SP 800-171–compliant operations. I understand that violations of the AUP may result in suspension or termination of access, notification to my PI or sponsor, and possible institutional or legal consequences.

## User Information

Name: _____

Institution/Organization: _____

Email: _____

TSCC Compliance Username (if assigned): _____

## Required Acknowledgments

[ ] I will protect my TSCC Compliance credentials and use Duo MFA for all logins.

[ ] I understand mobile devices are not permitted for accessing TSCC Compliance System.

[ ] I will store and process CUI/CAD within the authorized TSCC Compliance System only.

[ ] I will not attempt to bypass or interfere with TSCC Compliance security controls.

[ ] I understand my activity on TSCC Compliance CUI/CAD systems may be logged and monitored.

[ ] I will immediately report any suspected security incident or account compromise.

## Signature

Signature: _____

Date: