

American Science Cloud (AmSC) Acceptable Use Policy (AUP)

1. Purpose and scope

This policy governs access to and use of all computing, storage, data transfer, workflow, and network services provided by the DOE through the American Science Cloud (AmSC) and its Infrastructure Partners (IPs). It applies to:

- All users (including staff, affiliates, visitors, and collaborators),
- Principal Investigators (PIs), PI proxies/delegates, and project administrators,
- Any automated agents, workflows, gateways, or services acting on a user's behalf.

Use of AmSC constitutes agreement to this policy and to any applicable institutional user agreement(s), terms of award, or site-specific requirements.

This policy establishes baseline requirements for all participating American Science Cloud resources. Site-specific, service-specific, and program-specific rules may supplement this policy and, where more restrictive, shall control.

Users must comply with all applicable federal, state, and local laws and regulations; DOE orders, directives, and contractual obligations; institutional policies; and resource-specific requirements.

1.1 Definitions

For purposes of this policy:

- **Facility** means the American Science Cloud and its participating DOE Infrastructure Partners including NERSC, OLCF, and ALCF, their respective sites, and operators (LBNL, ORNL and ANL respectively).
- **Facility Resources** means computing, storage, data transfer, workflow, network, identity, and related services made available through the Facility.
- **User** means any individual or entity authorized to access or use Facility Resources, including through automated means.
- **Project** means an approved activity, allocation, award, proposal, or other authorized scope of work under which Facility Resources are used.
- **PI** means the Principal Investigator or equivalent project lead responsible for a project.

- **PI delegate / project administrator** means a person authorized by the PI or Facility to perform project administrative functions.
- **Automated agent** means any workflow, service, script, gateway, application, bot, service account, or other automated mechanism acting on behalf of a user or project.
- **Host institution** means a participating DOE laboratory, operating contractor, university, or other institution responsible for a Facility Resource.
- **Written authorization** means documented approval by the Facility or other authorized approving body in a form acceptable to the Facility or Facilities.
- **Sensitive data** means any information subject to legal, regulatory, contractual, institutional, or security handling restrictions beyond those approved for the relevant Facility Resource.

2. Facility mission: open scientific research

Facility Resources are intended to support open scientific research and work that is within the scope of an approved project and consistent with DOE User Facility objectives.

Unless expressly authorized in writing by the AmSC or Facility Director (or designee), Facility Resources must not be used to produce or support proprietary results and/or proprietary data.

Users are expected to use best efforts to publish results in open scientific journals or significant technical venues, consistent with the applicable user agreement and award terms.

The Facility recognizes that interim results, prepublication materials, software under development, and project-internal work products may remain nonpublic for limited periods consistent with applicable agreements, award terms, and policy requirements.

3. Authorization, review, and conditions of access

3.1 Review and approval

Use of Facility Resources is subject to review and approval by one or more of the following, as applicable:

- The UT-Battelle, LLC,
- The operating contractor(s) or managing institution(s) for participating Facility sites,
- The project PI (and PI proxies/delegates),

- The host institution(s),
- DOE and other state/federal agencies or funding entities.

The Facility may request supporting documentation to establish eligibility, project scope, or compliance, and may provide account/project information to authorized reviewers for these purposes.

3.2 Project scope requirement

All work performed using Facility Resources must be directly relevant to an active, approved project. Automated workflows/services must cease operation at project end or after any defined grace period.

3.3 Federated identity and institutional access

The Facility may support federated identity and trust arrangements that permit participating laboratories and institutions to accept authenticated users from other approved institutions, including employees of other laboratories, industries, or universities.

Access for foreign nationals may be permitted consistent with U.S. law, DOE requirements, site access rules, export control requirements, and host-institution procedures. Eligibility, identity proofing, sponsorship, onboarding, and access restrictions may vary by site and user category. Users must comply with all applicable facility-specific and site-specific access procedures.

Additional procedures governing federated identity, employee access across institutions, and foreign national access may be published separately by participating sites and shall apply as applicable.

4. Prohibited use (conduct and system integrity)

Users must not use Facility Resources in ways that are unlawful, unsafe, disruptive, or inconsistent with this policy, including:

1. Personal or private benefit
Facility Resources may not be used for personal, commercial, or non-project-related purposes.
2. Unauthorized access / impersonation / credential misuse
Users must not attempt to access accounts, data, or systems without authorization; must not impersonate others; and must not misuse credentials.

3. Circumventing security controls

Users must not bypass or weaken authentication, MFA, access controls, auditing, or network restrictions.

4. Reconstruction or reverse engineering without authorization

Users must not reconstruct, extract, infer, or reverse engineer restricted information, credentials, models, datasets, or software they are not authorized to access or analyze.

5. Unauthorized data modification or destruction

Users must not intentionally modify, delete, or damage information, filesystems, configurations, or services without authorization.

6. Malicious software and exploitation

Users must not introduce or run malware (viruses, worms, trojans), crypto-miners, botnets, or any code intended to exploit vulnerabilities or degrade service.

7. Denial of service or disruptive behavior

Users must not interfere with availability of Facility Resources or external systems, including excessive scanning, flooding, or abusive job submission patterns.

8. Penetration testing and vulnerability scanning

Security testing targeting Facility Resources is prohibited unless explicitly approved in writing under an authorized vulnerability disclosure or testing program.

Users who discover a suspected vulnerability must report it promptly through the Facility's designated security contact and must not further exploit, validate aggressively, or disclose it publicly without authorization.

9. Prohibited software

Certain software and use cases may be prohibited. Users must not download, install, or use prohibited software and must comply with changeable facility software/security controls.

10. Fair use and resource abuse

Users must use shared Facility Resources fairly and efficiently and must comply with scheduling, quota, rate-limit, allocation, and other resource management controls. Users must not evade such controls or submit workloads designed primarily to reserve, hoard, block, or unfairly monopolize resources.

5. Prohibited data

5.1 Default prohibition (applies unless an explicit written exception exists)

Users must not store, process, transmit, or remotely access any of the following on or through Facility Resources:

- Classified information (including, without limitation): Secret (S), Top Secret (TS), National Security Information (NSI), Secret Restricted Data (SRD), Special Access Program (SAP) data
- Controlled Unclassified Information (CUI) or equivalent restricted government data (including OUO/SBU/CTI where applicable)
- Export-controlled information (including ITAR-controlled and certain EAR-controlled codes/data)
- Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI)
- Personally Identifiable Information (PII) and Protected Health Information (PHI) (including data subject to the Privacy Act of 1974, HIPAA, or similar regimes)
- Proprietary information and trade secrets (unless explicitly authorized under a facility-approved proprietary program and written approval)
- Data, designs, or use that supports the design or development of nuclear, radiological, biological, or chemical weapons, or other weapons of mass destruction
- Any information whose handling requirements exceed the security authorization, approved operating posture, or permitted data types of the relevant Facility Resource

5.2 User responsibility for correct categorization

Authors/generators/owners of information are responsible for correct categorization and for ensuring that prohibited data are not introduced to Facility Resources.

6. Software and licensing

All software used on Facility Resources must be properly acquired and used in accordance with applicable licenses. Users must not possess, use, or transmit illegally obtained software or data, and must not copy/store/transfer copyrighted material except as permitted by the rights holder.

Users must comply with Facility requirements for containers, virtual machines, package repositories, third-party software sources, and other deployable artifacts, including any applicable provenance, patching, or vulnerability-remediation requirements.

7. Authentication, credentials, and account integrity

- Users must authenticate using an approved identity provider and MFA as required by the Facility/resource.
- Users must not share accounts, passwords, MFA tokens, SSH keys, API tokens, or other secrets.
- Collaboration/shared accounts are permitted only when explicitly provided and approved by the Facility (e.g., “collaboration accounts”) and must follow Facility rules.
- Users must promptly report suspected credential compromise or account misuse to help@amscproject.atlassian.net and follow remediation instructions.
- Users must maintain current contact information (email, affiliation, phone if required) and promptly update changes.
- Users are responsible for all actions taken using their accounts, credentials, tokens, keys, or approved automated agents.
- Service accounts, API credentials, long-lived tokens, and automation credentials may be used only as authorized by the Facility and must be protected, minimally scoped, and rotated or revoked when no longer needed.
- Secrets must not be embedded in source code, shared insecurely, or placed in public repositories or public workflow definitions.
- Automation should run under attributable identities where feasible, and users remain responsible for actions performed by workflows, gateways, agents, or services operating on their behalf.
- Access may be conditioned on explicit acknowledgment of this policy and periodic re-acknowledgment during account renewal, training, or access review cycles.

8. Monitoring, privacy, and administrator access

Facility Resources are government-owned/operated systems (or operated on behalf of the U.S. Government). To the extent permitted by law, users should have no explicit or implicit expectation of privacy. The Facility may:

- Monitor and log activity,
- Access files and communications as necessary for operations, cybersecurity, compliance, investigations, or legal obligations,

- Retain logs/traffic/files as required or permitted,
- Share relevant information with DOE, the operating contractor, incident response organizations, and law enforcement as appropriate.

9. Data management, stewardship, and retention

- The Facility may impose quotas and may remove data to protect operations, reclaim space, or comply with policy.
- Not all storage is backed up; users are responsible for appropriate backups, integrity checks, and lifecycle management of important data.
- Upon account deactivation or project end, the Facility may delete or reassign project data as needed, including transferring data to a PI or project administrator as appropriate.
- Some systems may employ automated purge policies on scratch/work filesystems; users must not rely on scratch space for long-term retention.
- Data handling, retention, purge, archival, transfer, and recovery practices may vary by resource and are governed by site-specific procedures where applicable.
- Data submitted to or created on Facility Resources remain the responsibility of the user, project, PI, and/or sponsoring institution except as otherwise provided by law, agreement, or policy.
- The Facility may access, preserve, transfer, disclose, quarantine, or delete data and related metadata as necessary for operations, cybersecurity, compliance, project continuity, records retention, legal process, or other authorized purposes.
- When a user departs, changes affiliation, or loses access, the Facility may maintain or transfer project data access to the PI, project administrator, or other authorized project personnel as appropriate.
- The Facility may preserve accounts, logs, files, and metadata beyond normal retention periods in response to legal hold, public records obligations, audit, investigation, subpoena, or other legal or administrative requirements.

10. Foreign national access and restricted parties

Foreign nationals may be permitted access consistent with U.S. law and DOE/site requirements. Access is prohibited or restricted for:

- Individuals/entities in embargoed countries,

- Persons on restricted party lists,
- Prohibited end-use activities, consistent with export control and federal requirements.

Access decisions may also be subject to identity proofing, sponsorship, institutional eligibility, citizenship/visa-related requirements where applicable, and site-specific onboarding procedures.

11. PI and project administrator responsibilities (project-level controls)

PIs (and approved delegates) are responsible for:

- Ensuring project usage stays within approved scope and allocations,
- Authorizing and periodically reviewing project membership and access needs,
- Ensuring workflows, gateways, and automation are developed and maintained securely,
- Preventing unauthorized access to project data and services,
- Cooperating with incident response and compliance reviews,
- Maintaining any required institutional agreements and project documentation where applicable.
- PIs and project administrators must ensure that project memberships, delegated roles, service accounts, and automated access methods are reviewed periodically and removed when no longer needed.
- Users, PIs, and project administrators must cooperate with incident response, forensic preservation, containment actions, credential resets, and temporary service restrictions when requested by the Facility.
- Any externally reachable services, persistent listeners, custom authentication services, or third-party integrations operated in connection with a project require prior Facility approval and must comply with Facility security, logging, patching, and vulnerability-management requirements.

12. Acknowledgment requirement (publications and presentations)

Users must acknowledge Facility Resources in publications and presentations that include work performed using them.

Required acknowledgment:

This material is based upon work supported by the U.S. Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, under the American Science Cloud project award number DE-SCL0000151 .

13. Warranty disclaimer

Facility Resources are provided “as is” and “as available,” without warranty of any kind, express or implied, including fitness for a particular purpose. The Facility is not liable for loss of data, corruption, or service interruptions due to hardware/software failure, misconfiguration, network issues, negligence, malicious actions, accidents, or other causes.

14. Enforcement, termination, and sanctions

Violations of this policy may result in actions including (but not limited to):

- Suspension or termination of access,
- Project suspension and/or allocation reduction,
- Administrative actions by the Facility or host institution,
- Referral to DOE or law enforcement where appropriate.

Access may be withheld or terminated at the Facility’s discretion for security, safety, operational, or compliance reasons.

The Facility may take immediate protective action, including suspension of accounts, jobs, workflows, network activity, or services, without prior notice when reasonably necessary to protect security, safety, compliance, evidence preservation, or operations.

15. Training, procedures, and policy updates

Users may be required to complete training, attestations, acknowledgments, or periodic renewals as a condition of access.

The Facility may publish procedures, standards, technical controls, and implementation guidance supporting this policy. Such materials may include, without limitation, requirements for identity proofing, federated access, foreign national onboarding, export control review, data handling, containers, user-operated services, incident reporting, and resource-specific operating rules.

The Facility may revise this policy and associated procedures from time to time. Continued use of Facility Resources after the effective date of an update constitutes acceptance of the revised policy.

16. Reporting misuse and security incidents

Users must promptly report suspected misuse, abuse, policy violations, or cybersecurity incidents to help@amscproject.atlassian.net.

Revision History

Version	Last Updated	Description
1.0	October 5, 2026	Initial version of the AUP