Cosmos Acceptable Use Policy

Effective Date: October 20th, 2025

Definitions

- **Cosmos**: NSF Category II Computing System managed at SDSC
- **User**: Any individual granted access to Cosmos system
- **PI (Principal Investigator)**: A User authorized to manage Allocations and Users on their Projects. A PI is considered to be an Allocation Manager and may appoint additional Allocation Managers
- **Allocation Manager**: A User role authorized by a PI to manage Allocations and Users on Projects
- **Project**: A collection of Allocations and Users managed by a PI
- **Allocation**: A provisioned amount and/or duration of a project
- **Individual Account**: An authenticated account assigned to an individual providing direct access to the resoure
- **Data**: All digital media or software stored or executed on the resource
- **Protected Data**: Data required to be maintained as private or confidential by applicable agreements, contracts, policies, regulations, or laws
- **Regulated Data**: Data subject to specific compliance requirements including but not limited to HIPAA, ITAR, EAR, CUI (e.g for dbGaP), FISMA, or PII
- **3rd Party Data**: Data not wholly owned by a Project's PI, Users, or the PI's employer or academic institution
- **Academic User**: Users affiliated with educational or non-profit research institutions
- **Industry User**: Users affiliated with for-profit entities or commercial organizations
- **MFA (Multi-Factor Authentication)**: Security process requiring multiple forms of verification
- **Export Control**: Regulations governing transfer of controlled information, technology, or materials to foreign nationals or entities

---

General Provisions

Individuals who receive access or an allocation to the Cosmos system are required to comply with this Acceptable Use Policy and all applicable institutional policies, federal, state, and local laws.

Cosmos system shall only be provided to individuals conducting:

- Legal and ethical research in recognized fields of study
- Work consistent with bona fide scientific research or approved commercial research agreements

- Activities authorized under executed service agreements or research contracts

---

User Responsibilities

Users shall:

1. Establish their identity through an approved Identity Provider prior to requesting an Individual Account
2. Reverify their identity and institutional affiliation and accept the latest version of this AUP at least annually
3. Only access and use Information Resources with explicit permission
4. Use Information Resources only to perform work and transmit/store data consistent with their authorized Projects and Allocations
5. Respect intellectual property and copyright laws and observe confidentiality agreements
6. Protect access credentials (e.g., username, private keys, tokens, passwords) issued for their sole use
7. Use unique, strong passwords and only enter credentials when logging into authorized Cosmos resources
8. Immediately report any known or suspected security breach, misuse of Information Resources, violations of policies, or disclosure of Protected Data to the Security Office
9. Comply with all applicable federal, state, and local laws, including Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), and HIPAA where applicable
10. Comply with Cosmos processes, procedures, controls, and directions from support personnel
11. Only use devices that are password protected to access Information Resources
12. Change passwords or re-create MFA tokens whenever there is suspicion of account compromise
13. Back up critical data using approved backup services

Users shall not:

1. Request or actively use more than one Individual Account
2. Request an Individual Account with false, invalid, or outdated identity or institutional affiliation
3. Share or release Cosmos-issued logins, MFA credentials, or passwords
4. Use Cosmos resources for financial gain (except as explicitly authorized under service agreements or research contracts)
5. Participate in copyright infringement, data theft, intellectual property theft, or any unethical, illegal, or inappropriate activity
6. Engage in activities that could disrupt or impede Cosmos operations
7. Create, transmit, or store illegal or inappropriate Data on Information Resources
8. Be paid or profit from non-sanctioned activities using Information Resources (cryptocurrency generation, etc.)

9. Attempt to access Information Resources not explicitly allocated or authorized
10. Attempt to circumvent security measures or controls
11. Attempt to scan or probe any Information Resource without prior authorization
12. Use Information Resources for work unrelated to the Project for which access was granted
13. Attempt to breach or circumvent administrative or security controls

---

User Eligibility and PI Responsibilities

All Users shall:

- Log into an approved Identity Provider when requesting an Individual Account
- Keep profile information current and accurate
- Maintain only one Cosmos account

A PI shall:

1. Provide evidence of work in their proposed field of study, and be an employee of the host institution
2. Apply for an Allocation to perform research on Information Resources
3. Only appoint eligible Allocation Managers to join their Projects
4. Ensure Users are trained on Cosmos and Project-specific processes, procedures, and controls prior to adding them to Projects
5. Be held accountable for the actions of their Projects' Users on Information Resources
6. Properly vet all users on their allocations, attesting that account credentials belong to the intended person

A PI and Allocation Manager shall:

1. Be currently employed and/or appointed by an eligible institution authorized to receive and execute research grants or have an executed service agreement with Cosmos
2. Maintain a valid email address from their current employer or academic institution
3. Only invite or admit eligible Users meeting at least one of the following identity criteria:
    - The PI or Allocation Manager has established a personal, academic, or professional relationship with the User
    - The PI or Allocation Manager has established a relationship with the User's academic advisor or supervisor
    - The User's email matches the domain of the specified institution
    - If the User's email does not match the institutional domain and the person is not personally known, the PI must document and verify the User's identity
4. Be responsible for all User activities on their Projects, Allocations, and Service Accounts
5. Authorize Users on their Projects to use, modify, destroy, share, or disclose Project-specific Data

6. Remove a User's access and report to the Security Officer if the User is no longer trusted, has misused resources, is suspected of illegal or unethical activities, or has failed to comply with this AUP
7. Ensure users with access via their allocation follow this AUP

Industry User Provisions

Industry Users receiving subsidized or free allocations shall:

1. Conduct research in an open manner with intent to publish findings
2. Publish research results in peer-reviewed journals, conference proceedings, or other publicly accessible venues within a reasonable timeframe
3. Make research methodologies and non-proprietary findings available to the broader scientific community
4. Acknowledge Cosmos support in all publications and presentations
5. Not assert proprietary claims that would prevent publication of research findings supported by free allocations

Industry Users under paid service agreements:

1. May conduct proprietary research as specified in their service agreements
2. Are subject to the terms and conditions of their executed contracts
3. Must comply with all technical and security requirements specified in agreements
4. May have different data retention and publication requirements as specified in contracts

All Industry Users shall:

1. Comply with all export control regulations and restrictions
2. Disclose all foreign national collaborators and international partnerships
3. Undergo export control screening for all international collaborators and company partnerships
4. Obtain appropriate export control licenses or authorizations before sharing controlled information
5. Not use Cosmos resources for work subject to export restrictions without prior approval and appropriate controls

---

Information Resource Access, Use and Security

Cosmos may terminate or modify a User's access to Information Resources for any reason at any time without notice.

Users shall:

1. Comply with Cosmos processes, procedures, controls, and directions from staff
2. Comply with Project-specific processes, procedures, controls, and directions from the Project's PI
3. Use Information Resources within the constraints of authorized Projects, Allocations, or permissions
4. Only create, transmit, or store Data directly applicable to authorized Allocations as permitted by current agreements, contracts, regulations, and laws
5. Respect the privacy of community members
6. Protect Cosmos, Users, and 3rd parties from misuse or theft of identity data, Project data, proprietary data, 3rd party data, or intellectual property
7. Only access Cosmos networks using approved entry points, processes, and methodologies
8. Securely maintain Cosmos-issued logins, credentials, and passwords
9. Only request refunds for jobs terminated due to Information Resource failures

Users shall not:

1. Use Information Resources in a manner not in compliance with Cosmos's mission, contracts, agreements, regulations, or laws
2. Request refunds for User application software failures

Data Management

While Cosmos endeavors to maintain the integrity of all research data and retain data beyond allocation periods on a best effort basis, Cosmos reserves the right to remove Data from Information Resources at any time without notice if:

- Misuse is detected
- Directed by a funding or law enforcement agency
- Directed by appropriate officials from the User's home institution
- The User or PI fails to maintain active allocations
- Stores compliant or restricted data

Use of resources and services through Cosmos is at your own risk. There are no guarantees that resources and services will be available, suit every purpose, or that data will never be lost or corrupted. Users are responsible for backing up critical data.

Data Ownership

Data created on Cosmos systems is considered the property of the PI and Project (subject to applicable rules from funding agencies and the PI's employment agreement), and Cosmos shall not assert additional intellectual property rights to this data.

PIs shall:

1. Control who accesses their Project's Data and may restrict or remove access at any time without notice
2. Control how their Project's Data is stored, copied, used, shared, disseminated, or transferred
3. Obtain all necessary rights and permissions to access, store, or use 3rd Party Data prior to uploading or using it on Information Resources

Users shall:

1. Comply with PI-specified rules on Data wholly owned by the PI, Project Users, or PI's employer or academic institution
2. Comply with all applicable 3rd Party Data agreements, contracts, policies, regulations, or laws
3. Own and be responsible for the Data they generate on or upload to Information Resources
4. Only use authorized software services to store and access Data on Information Resources

Users shall not:

1. Use, modify, destroy, share, or disclose Data without prior authorization from their PI
2. Have any expectation of privacy from authorized Cosmos staff on any Data they create, transmit, or store on Information Resources

---

Data Retention

- When a Project is terminated, all Project Data stored in the /home and /work directories shall be retained for 30 days
- When a Project is terminated or a User is denied access due to non-compliance with this AUP, all associated Data may be deleted at any time without notice

---

Protected and Regulated Data

CRITICAL: The baseline configuration of Cosmos is NOT designed to host regulated data (e.g., HIPAA, CUI, ITAR, etc.). Users intending to host regulated data must contact Cosmos team who will be redirected to appropriate resources that can handle such data.

Examples of Protected Data include but are not limited to:

- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Controlled Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Data subject to Business Associate Agreements (BAA)
- Technology Control Plans (TCP)
- Data Transfer Agreements (DTA)
- Data Use Agreements (DUA)
- Confidential Data Control Plans (CDCP)

Export Control Compliance

All Users must comply with U.S. export control laws and regulations, including but not limited to EAR and ITAR.

All Users shall:

1. Determine whether their research or activities involve export-controlled information, technology, or materials
2. Work with their organization and Cosmos to identify applicable export control constraints
3. Obtain necessary export licenses or authorizations before sharing controlled information with foreign nationals or entities
4. Immediately report potential export control violations to the Cosmos team

PIs with international collaborators or industry partnerships shall:

1. **Disclose all international collaborators** (both individuals and organizations) to the Cosmos team prior to granting access
2. **Disclose all company/industry collaborators** to the Cosmos team for export control screening
3. Complete export control screening for all international and industry collaborators before granting system access
4. Obtain Technology Control Plans (TCP) or equivalent documentation when required
5. Ensure all collaborators understand and comply with applicable export restrictions
6. Update the Cosmos team immediately if collaborator nationality, citizenship, or organizational affiliations change

Industry Users shall:

1. Undergo enhanced export control screening for all personnel accessing Cosmos resources
2. Disclose the citizenship and country of residence for all employees who will access Cosmos

3. Provide information about corporate structure, foreign ownership, and international operations as requested
4. Comply with deemed export regulations when foreign nationals access controlled information
5. Perform open publishable research when using Cosmos with unpaid allocation

Cosmos reserves the right to:

1. Deny access to any individual or organization that poses export control concerns
2. Require additional documentation, screening, or controls for international or industry collaborations
3. Immediately suspend access if export control violations are suspected
4. Report potential violations to appropriate regulatory authorities

---

Research Citations and Acknowledgments

Users shall reference Cosmos in any research report, journal, or publication that requires citation of work performed using Cosmos Information Resources. Recognition of resources is important for acquiring future funding for next-generation hardware, support services, and research & development activities.

Industry Users receiving free or subsidized allocations must acknowledge Cosmos support in all public presentations and publications resulting from work performed on the system.

Privacy and Data Logging

Logged information, including information provided for registration purposes, is used for administrative, operational, accounting, monitoring, and security purposes. This information may be disclosed, via secured mechanisms, only for the same purposes and to authorized parties.

Non-Compliance

Cosmos may terminate or suspend a User's access to Information Resources for failure to comply with this AUP at any time without notice.

Cosmos may take legal and/or disciplinary action in response to any User's unethical or illegal activity associated with using Information Resources.

Violations of this AUP may result in:

1. Written or verbal warnings
2. Revocation of access privileges to Information Resources
3. Deletion of User-owned Data from Information Resources
4. Reporting of User's activities to their PI, employer, academic institution, or applicable government or law enforcement agency
5. Civil or criminal prosecution

Activities in violation of any laws may be reported to the proper authorities for investigation and prosecution.

Agreement

By accessing Cosmos Information Resources, you acknowledge that you have read, understood, and agree to comply with this Acceptable Use Policy and all applicable laws, regulations, and institutional policies.

Contact Information: consult@sdsc.edu
