UNIVERSITY OF MIAMI

Frost Institute for Data Science and Computing
POLICY: Use of IDSC Computing Resources

Contents

1. Purpose

This policy establishes the governance framework for access, allocation, and responsible use of computing, storage, and data resources managed by the Frost Institute for Data Science and Computing. It is intended to support responsible data stewardship and alignment with sponsor expectations for internally and extramurally funded activities including federally funded research and educational activities.

2. Scope

This policy applies to University of Miami faculty, staff, and students; affiliated researchers; sponsored project personnel; and approved external collaborators. It governs all IDSC-managed technology platforms and associated services.

3. Policy Statement

IDSC resources are institutional research infrastructure assets. Use of these resources must support reproducible research practices, responsible data management, and compliance with applicable institutional policies and sponsor requirements.

4. Eligibility and Access

4.1 Project-Based Access. Access is granted on a project basis and requires an approved allocation and Principal Investigator (PI) or institutional sponsorship.

4.2 User Responsibilities. Users must comply with institutional Information Technology and security policies and any applicable sponsor and/or regulatory requirements.

5. Advance Commitment of Resources

5.1 Commitment Policy. Projects requiring guaranteed availability of compute (CPU/ GPU), storage, or data-transfer capacity must request advance commitments. These commitment requests will be evaluated on a case-by-case basis (see sec 5.2).

5.2 Review Criteria. Commitments are evaluated based on scientific and/or institutional priority, time sensitivity, resource availability, and funding/cost-recovery alignment.

5.3 Terms. Approved commitments will specify quotas, duration, renewal terms, and reporting or usage expectations.

5.4 Acknowledgement. PIs are required to acknowledge the use of resources in their grants and publications. Recommended language: "This work was conducted in collaboration with and/or using the computing and analytics resources of the University of Miami Frost Institute for Data Science and Computing."

6. Reservation and Scheduling

6.1 Shared Scheduling. Part of the computing resources will be dedicated under shared scheduling and the fair-share allocation model through standard resource management systems. While the shared scheduling model is generally first-come, first-served, IDSC reserves the ability to prioritize workloads that align with institutional priorities, sponsored commitments, or approved reservations.

6.2 Reservations. Reserved access may be approved for instructional events, coordinated workflows, or time-bound collaborations.

6.3 Reservation Requirements. Requests should be submitted in advance and must specify resource needs, time window, and justification aligned with outcomes.

7. Public and External Use

7.1 Institutional Priority. Primary access priority is for University of Miami research and educational activities and sponsored projects.

7.2 External Access. External access may be granted to academic, government, and industry partners under appropriate agreements intended to positively impact institutional priorities.

7.3 Conditions. External users must comply with all institutional policies, applicable sponsor requirements, and any data use, privacy, and Intellectual Property terms in governing agreements.

8. Cost Recovery and External User Charges

8.1 Service Unit. A Service Unit (SU) is defined as one CPU core hour or 2GB RAM per hour, whichever is larger, calculated per job OR 0.5 GB scratch space (as applicable to resource usage).

8.2 Cost-Recovery Model. IDSC employs chargeback models with costs approved by the Office of Research Administration (ORA) consistent with existing university policies. All users are billed under a cost-recovery model to support sustainability of infrastructure and operations. Cost recovery is required to ensure sustainability of shared infrastructure and compliance with federal cost accounting and institutional policies. For current UM and Non-UM Fee Schedules, please visit: idsc.miami.edu/fee-schedules.

8.3 IDSC Seed Grants. With a goal to expand collaborations in data science and computing, IDSC funds seed grants, and recipients are awarded a fixed allocation of SUs for a stipulated time. These grants-based computing (to the extent of the allocation) is funded by the Institute. Exceeding the allocation, however, will incur costs to be borne by the PI who received the seed grant award.

8.4 Computing for Coursework. With a goal to train the future workforce with computational competencies, IDSC provides grants to instructors that align hands-on training as a part of the coursework. Interested instructors should apply for a grant by providing course related information, deliverables, and requested resource requirements. Grants-based computing (to the extent of the allocation) is funded by the Institute. Exceeding the allocation, however, will incur costs and the instructor will be responsible for the related costs beyond the allocation.

8.5 External and Industry Users. External users, including industry members, are subject to full cost-recovery rates preapproved by the ORA (subject to change and every effort will be made to ensure the payees are notified of the changes at least 30 days in advance). These rates are reviewed periodically for consistency and to align with the prevailing cost of computing resources; priority or reserved capacity may incur premium pricing.

8.6 Billing. All usage must be associated with an approved funding source or contract. This requirement does not apply to: (i) students using resources for coursework (in compliance with Section 8.2); (ii) first-time users (e.g., research students, postdoctoral fellows, and early-career researchers) evaluating resources for application compatibility; and (iii) IDSC seed grant recipients (see Section 8.2). PIs who use student accounts to circumvent IDSC cost recovery policies will be deemed non-compliant. Such utilization will be classified as

research use and will be billed accordingly. Access to IDSC computing resources for the PI may be suspended until all outstanding charges are fully paid.

8.7. Storage Use and Data Retention Policy

This policy defines the appropriate use of storage resources within the IDSC Advanced Computing Services (ACS) environment. It establishes guidelines to ensure efficient utilization, system performance, data integrity, and equitable access. This policy applies to all users of ACS-managed computational resources, including faculty, staff, students, and authorized external collaborators.

8.7.1. HOME

Each user is allocated 250 GB of persistent storage for personal workspace. This space is intended for source code, scripts, small development datasets, configuration files, and libraries. HOME storage is quota-limited but highly reliable and designed for long-term retention.

8.7.2. PROJECT

PROJECT storage provides shared, medium-term capacity for applications and research data. It is intended for active research datasets, application I/O, and collaborative project data. A default allocation of 10 TB is provided per project and may be expanded upon justified request.

8.7.3. SCRATCH

SCRATCH provides 2 TB of high-performance, temporary storage for computational workflows. It is intended for intermediate data generated during job execution and must not be used for long-term storage or retention of inactive data.

8.7.4. SCRATCH Data Management Policy

SCRATCH storage is subject to periodic purging, with or without prior notice. Users are expected to remove data within 20 days or transfer required data to persistent storage. ACS is not responsible for data loss resulting from automated purge processes.

9. First-Time User Policy (Students, Early Career Researchers, and New Faculty)

9.1 Onboarding. First-time users must complete account provisioning, required onboarding/training, and acknowledgement of acceptable use and security requirements.

9.2 Starter Allocations. Uninitiated faculty members may receive starter allocation to help them evaluate suitability of IDSC computing resources for their computational research requirements.

9.3 Transition. Sustained usage requires a project allocation with an identified funding or cost-sharing mechanism.

10. Secure Enclave and Controlled-Access Data

10.1 Purpose. IDSC Secure Enclave is an isolated and dedicated computing environment to support controlled-access to sensitive datasets (e.g., dbGaP and similar repositories).

10.2 Compliance Alignment. IDSC Secure Enclave is designed to support security control expectations such as NIST SP 800-171 (or equivalent institutional standards), DUAs, and IRB requirements as applicable.

10.3 Data Handling. Users must access and use data for approved purposes only; data export and duplication are restricted and subject to controlled processes.

10.4 Access Controls and Monitoring. Access is limited to authorized personnel; enhanced authentication, monitoring, and auditing may be required.

10.5 Incident Reporting. Users and PIs must promptly report suspected incidents or policy violations through institutional IT/security reporting channels (e.g., UMIT Security Office).

11. Compliance and Enforcement

Failure to comply with this policy or applicable institutional/sponsor requirements may result in actions such as suspension or revocation of access, consistent with institutional policies and due process.

12. Policy Governance and Review

This policy is maintained by IDSC leadership and is reviewed annually or as required based on changes in infrastructure, security posture, and sponsor expectations.

13. Related Documents and Contacts

Related Documents: IDSC Acceptable Use Policy (AUP); institutional data governance guidelines; applicable project DUAs and IRB approvals.

Contact: Advanced Computing Services: https://hpc.idsc.miami.edu/

Frost Institute for Data Science and Computing (IDSC)
1552 Brescia Avenue, Coral Gables, FL 33146 | idsc@miami.edu 305.243.4962

Appendix A: Data Classification Levels (Operational Guidance)

Classification	Examples	Minimum Handling Expectations
Public	Open datasets; publicly shareable materials	No special restrictions beyond standard acceptable use.
Restricted	Institutional data requiring limited access	Access controls; least privilege; approved sharing only
Controlled	Controlled-access research data (e.g., dbGaP)	Secure Enclave required; DUA/IRB alignment; audited access; restricted egress
Sensitive	Data requiring highest protection (e.g., PHI)	Enhanced controls; encryption; monitoring; approved workflows; strict export controls

Note: Final classification and handling requirements may be determined by institutional governance, Institutional Review Board (IRB), and sponsor agreements.

Appendix B: Secure Enclave Access Workflow (Summary)

1. Submit Secure Enclave request with PI approval and project description.
2. Provide documentation (IRB approval, DUA, sponsor requirements) as applicable.
3. Complete required onboarding and security training.
4. Provision access with enhanced authentication and authorized user list.
5. Operate under monitoring/audit processes; request egress approvals when needed.