Acceptable Use Policy for Resources managed by the Research Cyberinfrastructure Center at UCI

Last Updated: October 2021

The purpose of the UCI Research Cyberinfrastructure Center (RCIC) and the resources it oversees is to further the scientific, research, and educational efforts of UCI and its partners. In general, any activity that interferes with this purpose may be modified or cancelled by RCIC staff. The resources can include computing, storage, web-server, databases, networking, and RCIC managed communication (email, discussion lists) and are called "research computing resources".

By using RCIC-managed systems and resources, you agree to the following Acceptable Use Policy:

1. University Policies

1.1 All users are responsible for following University of California's "Electronic Communication Policy" (https://policy.ucop.edu/doc/7000470/ElectronicCommunications) as well as any specific Departmental, College, or School requirements related to computing and electronics.

1.2 Principle of Community. All communications to and from RCIC should be conducted in a manner consistent with UCI's Principles of Community as articulated by our Chancellor at https://chancellor.uci.edu/vision/index.php. These include tolerance, civility, and respect for diversity of background, gender, ethnicity, race, religion, political beliefs, sexual orientation and physical abilities. True scientific and intellectual disagreement are celebrated and discussed openly. Abuse of any kind is not tolerated.

2. University Use Only

2.1 Research computing resources are specifically reserved for the use of scientists, researchers, staff, students, and defined outside collaborators to further the research and teaching mission of the university. Any use of the research computing resources for personal or commercial gain is strictly prohibited.

3. Remote Access

3.1 Remote access to RCIC infrastructure is only available through cryptographically-secure connections like ssh (secure shell), sftp (secure shell file transfer protocol), https (secured http), and others that encrypt connections end-to-end. Users may on connect to RCIC-provided and managed versions of these services.

3.2 SSH keys without password are not allowed. Some RCIC facilities allow users to place public ssh keys as authorized keys for access. In no instance may a user place a public key in their personal authorized keys configuration where the private key is passwordless. The only exception is a cluster-specific key that is used ONLY to authorize among nodes within the same cluster.

3.3 Tunneling/forwarding of local ports for remote access is only allowed through existing, secure, ssh tunnel mechanisms. No other mechanism for forwarding or exposing network ports is allowed.

3.4 Users may NOT store, utilize or install software that exposes internal ports through unsecured mechanisms like reverse-proxy (e.g., frp) that effectively bypass campus and/or RCIC firewalls. This type of software compromises the security of everyone.. *If such software is **utilized or stored** on any RCIC-managed file system, the user will have login rights removed for an unspecified period of time*. *Multiple occurrences will result in permanent ban.*

4. Maintenance

4.1 RCIC makes every attempt to schedule server and cluster maintenance during announced and specific maintenance time windows and to minimize impact. However issues do occur that may need to be handled outside these pre-described maintenance time windows.

5. Cluster Jobs

RCIC runs several clusters. The following applies to each one of these resources.

5.1 Cluster jobs must be run on compute nodes configured for this purpose. Running jobs on the login nodes is prohibited, and any jobs/processes that impact the performance or functions of the login nodes or interfere with other users running jobs will be terminated without notice.

5.2 Cluster jobs containing wait times or “sleep loops” beyond a reasonable period, may not be run. Any job with a long wait or that contains an impactful/sustained sleep loop may be terminated without advance notice.

5.3 Unattended listening services (jobs that create listening ports for other computers to connect to) are strictly prohibited, and may be blocked by RCIC Staff without notice. Users found to be utilizing such services may have their access privileges removed.

6. Quotas and Storage

6.1 Data Quotas. RCIC manages quotas on nearly all storage servers and can modify and enforce quotas on all user directories, including home, temporary/scratch, and group directories. Users are reminded that storage provided by RCIC is for research data only. Different storage locations have different policies for snapshot, backup, and retention; and users should be familiar with these location-specific policies. Users are responsible for ensuring that backups of their data exist.

6.2 Data Snapshots. While RCIC makes every effort to maintain the availability and integrity of our storage products, no data storage has historical backup. Some data servers provide "snapshot" capability where data changed/deleted within the snapshot window (usually less than 2 months) often can be retrieved. Notably, data in BeeGFS-based parallel file systems do NOT have the capability for snapshots.

6.3 Data Replication. RCIC is developing the capability to replicate all data it holds to an offsite location. Because of the volume of data, replication will be regular but is not likely to be daily. We treat RCIC data systems as having the primary copy of data. When data is changed/removed from the primary, any data in the replica (secondary) is eventually removed. Replication is not historical backup. Users requiring historical backup of data need to provide that capability for themselves.

6.4 Scratch Storage. Storage designated as “scratch” storage is valid only during a batch job and is automatically deleted when a job has completed. There is no large-scale, no-cost, long-term scratch available.

7. Software and Services

7.1 Software should directly support research/teaching. Users are generally *not restricted* from downloading/compiling software in their own home areas for use in their research or teaching. Users are responsible for the software they download or compile.

7.2 Users choosing to locally-install software have the responsibility to use software from trustworthy sources. These might include: common community repositories like CRAN, CPAN, PyPy, and Anaconda; community-acceptable applications; or known-to-the-user software projects. Users should refrain from downloading pre-compiled binaries or containers from unverifiable sources.

7.3 Requesting RCIC to install/compile software. User's may request RCIC to build/install software in system areas for community use. RCIC does not have the people resources to accept all requests and must prioritize. RCIC can also deny software that is unsuitable for the environment.

7.4 No guarantee of long-term maintenance of specific software/services. Systems software, security concerns, and other factors evolve over time and any of these changes may render a specific software/service to be unsuitable/unsupportable. Any such software will be removed from the infrastructure.

8. Licensing

8.1 Some software offered on RCIC resources is controlled by individual license agreements. Those license agreements may require restriction of access to only authorized individuals. Software installed on a central resource does not imply that the software is available to all users.

8.2 Some licensed software (.e.g. commercial compilers, licensed file systems) is funded directly by RCIC. However, most licensed software must be funded directly by the requesting group.

9. Restricted Data Sets

9.1 The following data cannot be stored on any RCIC-managed resources: HIPAA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act), PII (Personally Identifiable Information), PHI (Protected Health Information), CMMC level-3 regulated data or NIST 800-171 regulated data.

9.2 If you are using de-identified data where identifiers are held only on a non RCIC-managed storage system, then there is a high likelihood that this data can be stored on RCIC resources. Please contact RCIC for questions about suitability of storage for any specific data sets.

10. Cryptocurrencies, cryptographic mining, distributed cryptography

10.1 Performing "mining" operations involving cryptocurrencies such as BitCoin, Ethereum, Dogecoin, Chia Coin, and Filecoin, distributed cryptography such as the distributed.net projects, and all forms of volunteer computing such as SETI@Home are strictly prohibited.

11. Separation from the University

11.1 If you separate from the university (e.g., graduation, new job, retirement), RCIC will close your associated accounts and archive your data for a period of no shorter than 6 months.

11.2 If you own data space (e.g. on CRSP or DFS parallel file systems) and someone you have authorized to access this space separates from the university, all data in such space and owned by the separating user will revert to your ownership and control. It is your responsibility to notify RCIC when one of your authorized users has separated.

11.3 If you own data space (e.g. on CRSP or DFS parallel file systems) and you separate from the university, you MUST designate a new owner of the data space or all of it will be archived, including data that might still be owned by active users.

12. Amendments/Updates

12.1 Technologies and policies change over time. This acceptable use policy can be amended at any time and users are always bound by the most-recent applicable policy.

13. How to Acknowledge RCIC

13.1 Papers, presentations, and other publications featuring work that relied on RCIC resources, services or expertise should include the following acknowledgement:

This work utilized the infrastructure for high-performance and high-throughput computing, research data storage and analysis, and scientific software tool integration built, operated, and updated by the Research Cyberinfrastructure Center (RCIC) at the University of California, Irvine (UCI). The RCIC provides cluster-based systems, application software, and scalable storage to directly support the UCI research community. https://rcic.uci.edu

14. Violations of this Acceptable Use Policy or any other applicable University Policies

14.1 Violations of this policy or any other applicable University policies may result in the temporary or permanent removal of accounts associated with research computing.