Republic of the Philippines
Department of Science and Technology
ADVANCED SCIENCE AND TECHNOLOGY INSTITUTE

COMPUTING AND ARCHIVING RESEARCH ENVIRONMENT

Acceptable Use Policy (AUP)

This AUP is implemented by the COARE Team, in conjunction with COARE Service Level Agreement (SLA) and Data Policy.

Postal Address : Asti Bldg. UP Technology Park Complex, CP Garcia Ave.,Diliman, Quezon City 1101
Website : www.asti.dost.gov.ph
Email Info@asti.dost.gov.ph

Tel no. : +632 8249-8500
+632 8246-9755;
Fax no. : +832 8246-9764

Document version:
Version 9/ 1 July 2025

Version History

Version	Date	Description	Authors
0	22 November 2018	Draft Document	COARE Team
1	10 December 2018	Final Document	COARE Team
1.1	24 April 2019	Draft Document	COARE Team
1.2	24 May 2019	Draft Document	COARE Team
2	5 August 2019	Final Document	COARE Team
2.1	20 February 2020	Draft Document	COARE Team
2.2	4 June 2020	Draft Document	COARE Team
2.3	24 June 2020	Draft Document	COARE Team
3	7 August 2020	Final Document	COARE Team
3.1	26 May 2021	Draft Document	COARE Team
3.2	7 June 2021	Draft Document	COARE Team
4	14 June 2021	Final Document	COARE Team
4.1	16 August 2021	Updated Document	COARE Team
5	23 August 2021	Final Document	COARE Team
5.1	15 June 2022	Draft Document	COARE Team
5.2	22 June 2022	Draft Document	COARE Team
6	22 July 2022	Final Document	COARE Team
7	8 August 2023	Final Document	COARE Team
8	20 March 2024	Draft Document	COARE Team
8.1	30 April 2024	Final Document	COARE Team
9	18 March 2025	Draft Document	COARE Team
9.1	**1 July 2025**	**Final Document**	**COARE Team**

Contents

1.About this Document 4

2. Definition of Terms 4

3. General Conditions Use 7

4. COARE Acceptable Use Policy (AUP) 8

5.Responsibilities 11

6.Monitoring and Enforcement 12

7.Suspension and Termination of the Provision of COARE Services 12

Annex A: Prohibited Use and Content 14

Annex B: COARE Data Classification Guidelines 16

Annex C: List of Penalties 17

Annex D: List of Allowed Runs on the HPC Frontend 19

1.About this Document

The Computing and Archiving Research Environment (COARE) is one of the services offered by the Department of Science and Technology – Advanced Science and Technology Institute (DOST-ASTI) that provides computational and storage resources for research initiatives that address or contribute to the thematic areas under DOST's Harmonized National Research and Development Agenda (HNRDA) 2022-2028. COARE serves as a national-level supercomputing facility that provides platforms for data storage, analysis, and sharing through the following services: High-Performance Computing (HPC), Science Cloud, and Data Archiving.

This document is the Acceptable Use Policy (AUP) of COARE and is implemented to ensure the fair and equitable use of COARE and COARE services.

2. Definition of Terms

The following terms will be relevant as reference in understanding this SLA:

2.1 Accounts: This comprises the credentials and/or other applicable requirements that enable a COARE user to access COARE services. Account credentials include a unique username (following the format: "firstname.lastname"), password (if necessary), and other relevant information.

2.2 Batch: This is the COARE HPC's main partition dedicated to processing multi-core/multi-node CPU jobs in parallel.

2.3 COARE Data Catalog: A web-based research data repository that provides access to a collection of scientific datasets produced by various research findings.

2.4 COARE Services: This refers to the standard services that COARE offers, namely: High-Performance Computing (HPC), Science Cloud and Data Archiving.

2.5 COARE Service Level: The group of people that maintains COARE's operations, handles the provision of COARE services and provides support to COARE Users. The COARE Team is composed of four (4) levels of support:

a. 1st Level – L1 Support: Service Desk

b. 2nd Level – L2 Support: Technical Operations Team and Software Development Team

c. 3rd Level – L3 Support: Technical Operations Team Lead and Software Development

Team Lead

d. 4th Level – L4 Support: COARE Management

2.6 COARE Users: Users who have been given access to COARE, or have been provisioned with COARE resources, and/or use the COARE Services (HPC, Science Cloud and Data Archiving).

2.7 COARE Wiki: A platform for COARE users as their reference to any pertinent information related to COARE and any COARE services. Information such as the COARE Service Catalog, procedures in availing COARE services, Frequently Asked Questions (FAQs), templates, forms, and other relevant guides can be found in COARE Wiki.

2.8 Configuration Item (CI): Any managed component needed to deliver COARE services. CIs typically includes hardware, software, people, and documentation.

2.9 Data Archiving: A COARE service that provides a repository with redundancy that aims to accommodate various storage requirements of COARE users and to enable storing of data on a short-term or long-term basis. This does not include storage used in HPC (home and scratch) and Science Cloud (cloud disk storage).

2.10 Data Catalog Data Owner: A COARE User who is the rightful owner of a specific dataset in the COARE Data Catalog. Data Owners have the right to approve or reject Data Access Requests from End Users.

2.11 Data Catalog End User: A COARE user who has authorized access to datasets published in the COARE Data Catalog.

2.12 Data Classification: This refers to the Data Catalog's data classification categories/levels: Public, Private, Confidential.

2.13 Downtime: This is the period when a COARE service is not available during its agreed Service Availability.

2.14 Emergency Cases: Cases involving hardware/ facility failure, force majeure and/or security breach.

2.15 HPC: The COARE HPC Service consists of a cluster of compute and storage servers to allow high-speed and resource-intensive computations and processing of large datasets.

2.16 Home Directory (/home): The storage option recommended for storage of application source codes, user program binaries, user directories, modules directories, and small-sized active datasets.

2.17 Incident: An unplanned interruption to a COARE service or reduction in the quality of a COARE service.

2.18 Job: A job is an allocation of resources assigned to a COARE HPC user for a specified amount of time.

2.19 Job Script: This is a script created by users to submit jobs in the HPC. It contains job information and instructions on how the job will run in COARE.

2.20 Maintenance: An activity or series of activities conducted to keep COARE services operational and responsive after they are released and placed into production. This can either be scheduled (preventive) or unscheduled (corrective, emergency).

2.21 Metadata: The metadata contains the information (i.e., title, description, organization details, etc.) pertaining to dataset.

2.22 Node: A physical, stand-alone computer that handles computing tasks and runs jobs.

2.23 Resource Intensive Jobs: Jobs that require a large number of resources (related: see Annex D of this document for the list of allowed runs on HPC frontend)

2.24 Science Cloud: A COARE service that enables the provision of virtual machines (VM) for cloud-based applications and computing.

2.25 Science Cloud Dashboard (OpenStack): A web-based interface to manage virtualized resources in the Science Cloud.

2.26 Science Cloud Project: A user or resource partner in COARE Science Cloud that is used to isolate compute resources (CPU, memory, disk and object storage, network, user/user-group access, etc.)

2.27 Scratch Directories (/scratch): These directories are intended for the storage of the user's running jobs, especially for execution of heavy I/O operations.

2.28 Service Availability: The ability of a CI or a COARE service to perform its agreed upon function when required. This is often calculated based on agreed upon service time and downtime.

2.29 Service Failure: This happens when the intended quality of service (e.g., uptime, queueing, support acknowledgment target, resolution target, etc.) is not being attained and, as a result, committed service level and service delivery cannot be provisioned.

2.30 Service Request: A request from a user for information about, change in/to, or access to a COARE service.

2.31 Ticket: A ticket is a general term used to refer to a record of work performed/addressed or to be performed/addressed by the COARE Team. For a more efficient service delivery and support, COARE users are encouraged to submit service requests and report incidents by logging a ticket through the COARE User Portal

2.32 Uptime: The period when a system has been running and when a COARE service is available during the agreed Service Availability.

2.33 User Portal: The main platform that the COARE Team use to carry out service request management and incident management processes. All service requests and incidents concerning any COARE service must be logged through a ticket in the COARE User Portal.

2.34 Virtual Machine (VM): A virtual server provided through the COARE Science Cloud service for cloud-based applications and computing.

2.35 Waiting Time: The span of time a submitted job takes before it changes its state from "Pending" to "Running".

3. General Conditions Use

The following outlines the general conditions of use of COARE:

a. The use of COARE is intended to support research and development (R&D) work and other scientific studies only. Users are expected to be responsible in using COARE in an efficient, effective, ethical, and lawful manner. See Annex A of this document for a detailed list of provisions on Prohibited Use and Content.
b. Users are expected to access COARE only with proper authentication credentials provided by the COARE Team. Users should be responsible for their credentials. For newly approved account applications, the COARE Team will issue an individual account with a temporary password to each first-time COARE user.
c. Users are encouraged to notify the COARE Team of any update on their contact details as soon as possible. This is to ensure that all correspondence sent by the COARE Team will only be delivered to and received by authorized COARE users.
d. Users are to submit all their requests (service requests and incident support requests) through logging of a ticket in the COARE User Portal.
e. Users are encouraged to treat COARE as an alternative storage option and to secure a copy of their data regularly to ensure no data loss. COARE should not be intended as the sole data repository of COARE users.
f. Users are to cite or acknowledge the DOST-ASTI and corresponding Data Owners (if applicable) in any paper, publication, presentation, or any other related content which resulted from research that has utilized the COARE Services and/or datasets especially those published in the COARE Data Catalog. Likewise, users are expected to provide an acknowledgement text (e.g., "This research was carried out in part using the DOST-ASTI's COARE") in their paper or any research output once they have finished their research. DOST-ASTI, COARE and/or PREGINET's logos must also be included in any case they have a website.
g. Users are encouraged to furnish the COARE Team with a copy of their research output (e.g., abstract, thesis, research paper, presentation slides, journal/news/feature articles, interviews, video presentations, etc.).
h. The DOST-ASTI, through the COARE Team, has the sole discretion to determine whether a user's use of the COARE Services violates the COARE's policies (see Annex A of this document). All content that is provided to the DOST-ASTI through COARE, or actions that are performed via a user's account, whether provided by or performed by the user and other end-users (if any), are the sole responsibility of the user.

4. COARE Acceptable Use Policy (AUP)

I. General Policies on the Usage of the COARE HPC Service

a. To utilize the COARE HPC, users will be provided with a COARE account which will be valid depending on the agreement between COARE and the partner. Account validity may be extended by applying for account renewal (via renewal of Memorandum of Agreement and account renewal form for individual users only), subject to the COARE Team's evaluation.

b. Once their application is approved, new COARE HPC users will be issued an individual account with a temporary password. Users should change their temporary password after their first successful login to COARE.

c. The COARE account is protected by the user-supplied public/private key pair that are both for the sole use of the COARE user and should not be used by or shared with other people or groups. Users are expected to be responsible for their credentials and/or private key in accessing COARE.

d. Any requests for an allocation increase will be subject to the COARE Team's evaluation and approval.

e. The /home directory should only be used for user's files (e.g., final research output, scripts, datasets, etc.) and the scratch directories should only be used as storage for active data and running jobs.

f. Both the /home directory and the /scratch directories) should not be used for long-term storage.

g. The frontend can only be used for copying files and as a jump-off server to connect to compute nodes (See Annex D for allowed runs on the HPC frontend.) Users are strictly prohibited to run resource-intensive jobs on the front-end (see Annex C for penalties)

h. Users can compile and install applications that will not require administrative privileges only on their home directories. However, it is recommended that compilation and installation of applications in the HPC are done by the COARE Team.

i. If the software that the user needs require a license, the user will be asked to provide the necessary license. Once the software is installed, users may choose to share the software with their colleagues and other users of the HPC.

j. The COARE Team will be conducting storage audit activities regularly as part of COARE's maintenance activities to manage the capacity and maintain the availability of COARE's resources. Data purging may be performed based on storage audit findings. Data purge schedules will be announced via email.

k. For expired HPC user accounts, notice to purge users' files (stored in the home and scratch directories) will be sent by the COARE Team upon expiry of users' account. Users will be given ninety (90) calendar days to back up their files upon expiry of their account. On the 90-day mark, the COARE Team will proceed with the deletion of ALL files of expired accounts.

II. General Policies on the Usage of the COARE Science Cloud Service

a. To utilize the COARE Science Cloud, users will be provided with a COARE account which will be valid depending on the agreement between COARE and the partner. Account validity may be extended by applying for account renewal (via renewal of the Memorandum of Agreement), subject to the COARE Team's evaluation.
b. Once their application is approved, new COARE Science Cloud users will be issued with the necessary credentials to access COARE. Users should change their temporary password after their first successful login to COARE.
c. Any requests for an allocation increase will be subject to the COARE Team's evaluation and approval.
d. The COARE Science Cloud may be used for cloud-based applications and computing. Users are expected to utilize the virtual resources provided to them for R&D purposes only.
e. The COARE Team has the right to shut down a virtual machine (VM) or disable the network connectivity of a VM if said VM is conducting or is involved in malicious activities.
f. Users have full control of the resources allocated to them. They should be responsible for conducting measures to manage (i.e., instantiating VMs, deleting volumes, creating volume backups, etc.), optimizing, and secure (i.e., creating security groups and OS-level firewall) the virtual resources allocated to them.
g. The COARE Team will not be liable for retrieving files or data that have been deleted due to users' negligence (e.g., weak passwords, insecure SSH authentication methods, etc.) and/or compromised through hacking, worms, etc.
h. Users must create a virtual local area network (LAN) in instantiating a VM. (See COARE Wiki).
i. Users should secure their own backup through the Science Cloud Dashboard.
j. The COARE Team will be conducting storage audit activities regularly as part of COARE's maintenance activities to manage the capacity and maintain the availability of COARE's resources. Data purging may be performed based on storage audit findings. Data purge schedules will be announced via email.
k. For the expired Science Cloud user accounts, the COARE Team will send a notice to purge users' VMs upon account expiry. Users will be given ninety (90) calendar days to back up their VMs upon expiry of their account. Unless users apply for renewal of their account, the COARE Team will proceed with the deletion of ALL Science Cloud resources of users with expired accounts on the 90-day mark. However, VMs of expired accounts belonging to a Science Cloud Project with at least one (1) active account will be exempted from purging.

III. General Policies on the Usage of the COARE Data Archiving Service

1. The COARE Data Archiving Service is intended for long-term data storage and distribution
2. **Specific AUP provisions on the Data Catalog: Data Owner**
    a. While there is no default allocation set in the Data Catalog for Data Catalog Owners, provision of resources for the Data Catalog will be based on the COARE Team's evaluation and recommendation.
    b. Data Owners shall hold exclusive rights over their datasets published in the Data Catalog. Thus, it is their duty to grant or deny data access requests for Privat and Internal datasets submitted by Data Catalog End Users.
    c. Data Owners are only allowed to upload datasets that are appropriate for research and development (R&D) work and other scientific studies. Storing data that is unrelated to research (e.g., documents, viruses, and media files such as movies, music, and photos not related to research) is prohibited**.**
3. **Specific AUP provision on the Data Catalog: End User**
    a. To utilize Data Catalog, an End User will be provided with a Data Catalog account which will be valid for 3 months.
    b. Except for public datasets, End Users will only be able to access or download datasets published in the Data Catalog with appropriate permissions from Data Owners.
    c. End Users who want to download datasets classified as Private may submit their request through an accomplished COARE Data Catalog Data Access Request Form.
    d. End Users who want to download datasets from the Data Catalog must duly comply with and agree to the COARE End User License Agreement (EULA), as well as with any additional license agreements provided by the Data Owners.

5.Responsibilities

Responsibilities of COARE Users

a. Abide by all policies (SLA, AUP, and Data Policy) issued by the COARE Team governing or concerning COARE Services;
b. Provide all the necessary details (e.g., screenshot of logs, name of Science Cloud Project, IP address of VM) or their service request or encountered service failure;
c. Handle the cost of licensed software needed for a user's project/s;
d. Report any issues encountered (e.g., service disruption, service failure, bugs, malfunction, degraded performance, etc.);
e. If users discover a bug and/or exploit that potentially bypasses admin controls/ or enables unfair advantage over other users, users are expected to report it immediately to the COARE Team;
f. Utilize the COARE User Portal in logging service requests and reporting incidents;
g. Cite or acknowledge the DOST-ASTI in any paper, publication, presentation, and other related content which resulted from R&D activities that utilized the COARE Services. DOST-ASTI, COARE and/or PREGINET's logos must also be included in any case they have a website.

Responsibilities of the COARE Team

a. Meet the identified service level targets;
b. Monitor the operations of COARE regularly and respond accordingly as soon as any service disruption, degradation, or failure has been detected or made known;
c. Send appropriate notification to COARE users concerning all scheduled and unscheduled maintenance;
d. Inform the users of the nature of any service failure that is occurring and may occur, as well as the estimated service restoration timeline or resolution time, if possible;
e. Communicate important updates and notify COARE users once service disruption, degradation, or failure has been resolved;
f. Comply with any requirements mandated by existing laws and policies (i.e., COARE AUP, COARE Data Policy);
g. Notify COARE users of any changes made to COARE's policies, procedures, and new services or features that are added to the existing COARE Services;
h. Recommend best practices on COARE Services usage and facilitate moderation of fair usage of the shared COARE Services among COARE users;
i. Ensure that usage of COARE Services will solely be for R&D purposes only;
j. Direct the COARE users to the COARE User Portal for a more efficient service delivery and support concerning their service requests or incident support requests.

6.Monitoring and Enforcement

While not obliged to perform investigations, the COARE Team may conduct the following monitoring and enforcement activities in accordance with the terms of this AUP:

a. Investigate violations of the AUP and misuse of COARE Services.
b. Investigate and help prevent security threats, fraud, or other illegal, malicious, or inappropriate activity.
c. Remove, suspend access to, or modify any content or resource that the COARE Team believes to be in violation of this AUP or any other agreement the COARE Team has with the User on the use of COARE Services.
d. Suspend access to COARE and terminate provision of COARE Services to users for usage that is in violation of this AUP.
e. If the COARE Team decides to push through with the suspension or termination of COARE access or provision of COARE Services, a one-month notice prior to the suspension and/or termination will be sent to the user.
f. Unless overruled by a superseding decision from the COARE Team or an agreement between the COARE Team and the user, the announced suspension and/or termination will take into effect a month after the notice has been sent.

7.Suspension and Termination of the Provision of COARE Services

This section outlines the provisions on the suspension and termination of a user's access to COARE:

I. The COARE Team may suspend access to COARE and terminate the provision of COARE services to a user if:

a. The COARE Services have been used, are being used, or are planned to be used by the user in violation of this AUP.
b. There is refusal to cooperate on investigations of any suspected or proven violations of this AUP that have been observed.
c. The COARE Services provided to the user have been manipulated by a third party, in violation of this AUP.
d. The suspension of access and the provision of COARE Services are necessary to protect the entire COARE, its network infrastructure, and other COARE users.
e. The continued use of the COARE Services by a user may adversely impact the entire COARE, the COARE Services, other COARE users, the COARE Team, and the DOST-ASTI.

II. The COARE Team shall issue a notice of suspension to the user to allow time to resolve the grounds on which the suspension is based, unless the COARE Team determines that either suspension on shorter or contemporaneous notice or immediate suspension without notice will be necessary to protect COARE, its users, or any third party from operational, security, or other risk, or the suspension is ordered by a court or other judicial body.

Annex A: Prohibited Use and Content

COARE users are prohibited from using COARE resources in a manner that the COARE Team believes to be:

1. Unrelated to R&D activities;
2. In violation of any local, state, national, foreign, or international statute, regulation, rule, order, treaty, or other pertinent laws;
3. Abusive, deceptive, pornographic, obscene, defamatory, slanderous, offensive, or otherwise inappropriate or illegal;
4. In violation of or is encroaching on the rights of others, including, but not limited to, infringement or misappropriation of any intellectual property or proprietary right of another;
5. An impersonation of any person or entity or otherwise misrepresents a COARE user's affiliation with a person or entity;
6. A modification of any software included in the COARE Services, except to software/applications included in the COARE Services that have been provided to or acquired by a COARE user under a separate license that expressly permits the modification of software/applications;
7. A means to reverse-engineer, disassemble, or decompile the COARE Services or software/application included in the COARE Services, except as required by local law and as granted by the COARE Team;
8. An interference, disruption, or degradation to the COARE Services, other COARE users' access to COARE and usage of the COARE Services, or equipment or networks connected to the COARE Services;
9. A means to violate the security and integrity of a system, including, but not limited to:

    a. Accessing or using any system, whether through hacking, password mining, or any other means, including attempts to probe, scan, or test the vulnerability of a system or to breach any security or authentication measures used by system, without permission granted by the COARE Team;
    b. Monitoring data or traffic on a system without permission granted by the COARE Team;
    c. Forging packet or email headers, or any part of a message describing its origin or route,
    d. Intentional uploading of malicious content (such as those that contain viruses, worms, corrupt files, trojan horses, or other forms of corruptive code, or any other content that may compromise the Services);
    e. Hacking, destabilizing, or adapting the COARE Services, or altering another website to falsely imply its affiliation with COARE and the COARE Services;
    f. Activities that connect to any users, hosts, or networks where COARE users do not have permission to communicate with (i.e., users, hosts, or networks);
    g. Monitoring or crawling a system so that such system is impaired or disrupted;

h. Intentionally interfering with the proper functioning of any system, including any deliberate attempt to overload a system by any means (e.g., distributed denial-of-service attacks, etc.);
i. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

Annex B: COARE Data Classification Guidelines

The COARE implements three (3) levels of data classification:

1. **Public:** All data classified as Public are accessible and are available for download to anyone who has a registered account in the Data Catalog. There are no other permissions, requirements, or Data Access Requests needed for the downloading of public datasets
2. **Private:** All data classified as Private belongs to the rightful Data Owner who chooses to share their data with only a select few. The titles of Private datasets, however, are still viewable and the metadata are still indexed. Access to Private datasets can only be provided through an approved Data Access Request Form. If the Data Owner approves the Data Access Request, the End User will be able to download the Private dataset requested.
3. **Confidential:** All data classified as Confidential are not shared and are not included in the COARE Data Catalog's list of datasets that can be accessed by End Users. Confidential datasets belong to the rightful Data Owner/s who, by reason of security, choose not to share or enable public access to their data. Data access requests will not be accommodated for Confidential datasets, and the existence of these datasets will not be displayed in the Data Catalog. Thus, Confidential data will not be viewable to anyone except to the COARE Data Catalog system administrators and the exclusive Data Owners themselves.

Annex C: List of Penalties

The COARE Team will impose the following penalties on violators of COARE AUP sections:

HPC

Running resource-intensive jobs on the HPC frontend.

COARE Users who ran their jobs on the frontend (without using SLURM) resulting in slowing down or inaccessibility of the service.

	Actions
1st offense	Email reminder from the COARE Service Desk including possible consequences and wiki link of the best practices.
2nd offense	Kill running job/s on the frontend
3rd offense and subsequent offense	Disable account for five (5) days
	Kill running job/s on the frontend

Sharing of Accounts

COARE users who shared their HPC account/s with other people or group.

	Actions
1st offense	Email reminder from the COARE Service Desk including possible consequences.
2nd offense	Disable accounts of users sharing accounts.

Running non-research related jobs.

COARE users who used HPC for non-research related jobs like crypto mining, personal runs, etc.

	Actions
1st offense	Email reminder from the COARE Service Desk.
	Disable accounts of users sharing accounts c/o COARE Technical Operations Team.

Using the service for illegal, malicious, or inappropriate activity

Hacking, password mining, and the likes (Annex A, Section 9)

	Actions
If proven	Disable the network connectivity of the VM
	Email notification from the Service Desk
	Disable user's account bypassing the 1-month notice rule
	COARE Team shall also determine if the user will be banned from re-applying to use any of the COARE services.

Science Cloud

Sharing of accounts

COARE users who shared their Science Cloud account/s with other people or groups.

	Actions
1st offense	Email reminder from the COARE Service Desk including possible consequences.
2nd offense	Disable accounts of users sharing accounts.

Using the service for illegal, malicious, or inappropriate activity

	Actions
If proven	Disable the network connectivity of the VM
	Email notification from the Service Desk
	Disable user's account bypassing the 1-month notice rule
	COARE Team shall also determine if the user will be banned from re-applying to use any of the COARE services.

Data Archiving

Data Owners: Using the service for illegal, malicious, or inappropriate activity.

	Actions
1st offense	Email reminder from the COARE Service Desk.
2nd offense	Email notification from the COARE Service Desk to revoke user's account and deletion of stored data.

End User: Using the service for illegal, malicious, or inappropriate activity.

	Actions
1st offense	Email reminder from the COARE Service Desk.
2nd offense	Revoke account

Annex D: List of Allowed Runs on the HPC Frontend

Only those activities that use minimal compute resources (such as CPU, memory, and network bandwidth) are allowed on the HPC frontend, such as (but not limited to) the following:

1. Manipulating files and directories
2. Viewing and editing files
3. Downloading and uploading files from the internet
4. Extracting and /or compressing files
5. Checking user information
6. Managing jobs
   - Viewing information about Saliksik nodes and partitions (sinfo)
   - Submitting SLURM script to the queue (sbatch)
   - Viewing of jobs information (squeue, scontrol)
   - Cancelling of submitted jobs (scancel)
7. Checking of modules
   - Viewing of existing and currently loaded modules
   - Viewing of information about the modules
   - Loading or unloading of modules
8. Showing installed packages or applications of a module
   - R, Anaconda, Matlab, and the like.