Access and Usage Policy for ACE HPC (Compute and Storage Resources)

Version: 1.0
Effective date: 10/11/2023
Date of Next Review: 09/11/2025

Author: Ronald Galiwango
Contributors: Grace Kebirungi, Mike Nsubuga, Daudi Jingo and Christopher Whalen

Table of Contents

1 Introduction

In 2019, the Infectious Diseases Institute (IDI), Makerere University's College of Computing & Health Sciences in partnership with the US Government National Institute of Allergy and Infectious Diseases and the Office of Cyber Infrastructure and Computational Biology(NIH/NIAID/OCICB) established the African Center of Excellence in Bioinformatics & Data Intensive Sciences, one of the only 2 such centres on the African continent, the other located in Mali. Since its establishment in 2019, the ACE has assembled a variety of computational facilities.

The ACE computational facilities encompasses its hardware (a high performance computing cluster (HPC), a data centre (data storage facilities), a tele learning centre (audio-visual and networking facility), a Virtual Reality room (Visualisation Lab) and a 3D printer), software, network connections and data. Failure to use these resources properly may result in various penalties, including, but not limited to, loss of access, administrative, academic, civil and/or criminal action.

The ACE advances research in Uganda and Africa at large by administering a state-of-the-art cyberinfrastructure, providing sustainable research services, and facilitating an interdisciplinary approach to the development and application of advanced computing and data processing technology throughout the research community and provision of data storage infrastructure.

The ACE is staffed by a team of research scientists, software developers, and a systems administrator with expertise in supporting high performance computing (HPC) and computationally dependent disciplines.

Below is a list of user requirements and responsibilities, general use policies, procedures, and security rules that apply to individual end users of the ***HPC (For the purposes of this policy the initials "HPC" includes all systems operated by ACE including Compute and Storage Resources such as virtual machines, VPN concentrators, workstations, HPC, virtual reality equipment, and any other platforms)***. The policy applies to all Infectious Diseases Institute (IDI) staff, non-staff from the Makerere University Research Community and Uganda at large, foreign nationals (such as visiting scholars and external users from abroad), students and all end-users who shall by nature of their work need to use or visit the facilities. These policies include any parts, items and all related input, processes, software, hardware, facilities and or stored data with the ACE computational facilities.

It is important to note that these policies are neither exhaustive nor exclusive. The fact that a certain action is not mentioned does not imply that it is permitted, nor, for that matter, prohibited. Before doing such an action, the user needs to check with the ACE Service Desk (support@ace-bioinformatics.org) and wait for confirmation.

2 Access and Usage Policy

Access is granted for research and education that meets the objectives of the ACE program and can be revoked at any time if users do not adhere to the terms of use or the policy as detailed in this document. The ACE infrastructure provides a suite of services that includes Virtual Reality, HPC, Virtual Machines, and Kubernetes.

2.1 Requirements

2.1.1 Authorisation

Matriculated students and faculty in the Bioinformatics program can request accounts. Other users must be part of an approved project with a Principal Investigator who must sponsor their account on the ACE infrastructure and then be approved by the ACE director or authorized delegate. Authorisation to access ACE Computational Facilities is given via ACE User registration upon which a user account is created. As part of this process users must have read the ACE HPC User Policy and completed appropriate training.

2.1.2 Obtaining a User Account

To get an account on the ACE HPC, a prospective user should follow an application process outlined below:

- Applicants need to send an email to support@ace-bioinformatics.org and in response, they are required to fill a request form containing information about their research goals, technical requirements including CPU core hours and storage, scientific programming needs and HPC experience.
- New proposals will be reviewed weekly and outcomes reported to applicants (for those requesting for a waiver) or quotations sent otherwise.
- Applicants should consider and indicate training requirements as this aids the ACE team in prioritizing and scheduling training workshops.

2.1.3 Valid Contact Email

Every account is required to have a contact email address that is associated with it. Email is used as the primary communication channel between ACE@HPC and the user.

2.1.4 Subscription to the ACE HPC Users Mailing List

While an account is active, the user is required to subscribe to the ACE users mailing list. This list is used to notify everyone of important changes and events such as training, software updates, scheduled maintenance updates etc. List membership is automatic upon creation of the account, and persists until the account is deactivated.

2.1.5 Training

Prior to account access activation, each new user is required to attend/complete whatever training is specified by the project of training that is dependent on the resource requested and a certificate of completion issued. All new users are required to complete new user training in addition to other resource request dependant training.

2.1.6 Usernames and Passwords

A unique user identifier (username) and an associated password are required of all ACE HPC users. All passwords must conform to the ACE HPC guidelines.
Passwords must follow the minimum strength policies per guidance below:

- Consist of a minimum of 14 characters.
- Use a random mixture of upper and lower case letters, numbers, and symbols (but remember that you may need to enter it on a tablet or a smartphone).
- Avoid dictionary words, names, dates or common phrases.
- Avoid simple sequences or keyboard patterns such as “qwertyuiop” or “23456789”.

2.1.7 Access to the HPC cluster

Access to the HPC Linux cluster is to be via Secure Shell protocol (SSH) to respective login nodes or other interfaces that may be intended for direct access (e.g. Web Portals) and all access to compute nodes must be via the job scheduler (**SLURM**). Direct access to compute nodes is not permitted. A maximum number of concurrent login sessions will be enforced on login nodes. SSH sessions that have been idle for an amount of time will be automatically disconnected. These limits will be adjusted as necessary to manage login node resources and to comply with applicable security standards.

2.1.8 Remote Access Policy

Access to the platform from offsite of ACE-IDI is only allowed via encrypted VPN and use a multifactor token which may be a physical token or a virtual token used with one-time password software installed on a smartphone. When account entitlement ends, the HPC user’s token will be disabled. Physical tokens remain the property of ACE and must be returned upon completion of approved activities.
It is not necessary for the remote device (defined as any laptop, tablet or PC) to be managed by ACE, however;

- ACE requires users to be responsible for the deployment of firewalls, anti-malware software and automatic updates on remote devices that they use to connect to the ACE HPC, all of which should be up to date.
- ACE requires users to be responsible for the associated risk of connecting from public networks and to act with care in public places to avoid the risk of screens and confidential notebook computer activity being overlooked by unauthorised persons.
- ACE requires users are responsible for the deployment of the usernames and passwords on their machine. Passwords should follow the guidelines in the password section below.
- ACE users will connect to ACE HPC using secure encrypted connection.

2.1.8.1 ACE Cyberinfrastructure Use by Foreign Nationals

ACE Uganda was launched as a regional platform to enable science. Its use by foreign nationals is generally permitted regardless of whether access to ACE HPC resources is from within Uganda or abroad. Foreign nationals have to comply with all ACE usage policies, local and government of Uganda policies and regulations on national security.

2.2 User Responsibilities

2.2.1 Individual Account Management

Access to the HPC@ACE is via password protected personal accounts that are created by ACE admin. You have the responsibility to protect your account from unauthorized access, and for the proper expenditure of allocated resources. Users are expected to follow standard security practices to ensure the safety and security of their accounts and data. (See the Data & Security sections below). Policies regarding account creation and access to HPC resources are subject to change.

2.2.1.1 Maintaining an up-to-date Contact Email

Every user is responsible for keeping the supplied contact email address that is associated with their account up to date. In the event that an address is discovered to be invalid, the associated user account will be locked. HPC users should promptly inform ACE of any changes in contact information.

2.2.1.2 Account Sharing

Users may not share their account(s), password(s), personal identification numbers, security tokens, or similar information or devices used for identification and authorization purposes. Your account is for your use only. It is not to be shared with others; neither students nor other collaborators. Others who need access must request their own account. Under no circumstances may any user make use of another user's account.

2.2.1.3 Account Passwords

Every account is associated with a password which serves as the key to account access. You are responsible for protecting your password from authorized access. Don't write your password where it can be easily found by others. Users are advised to change their passwords periodically to ensure the security of their accounts. Passwords must not be shared with any other person and must be changed as soon as possible upon suspected compromise, or at the direction of ACE personnel. Password change policy every 180 days

2.2.1.4 Mailing List Membership

Mailing List membership is automatic upon creation of the account, and persists until the account is deactivated. Anyone wishing to be removed from the list should send an email to support@ace-bioinformatics.org and request that their account be terminated.

2.2.2 Fair (Acceptable) usage policy

2.2.2.1 Reporting Suspicious Activity

ACE personnel and HPC users are required to address, safeguard against, and report misuse, abuse and criminal activities and all violations of the ACE HPC Policy to the ACE HPC Help Desk (support@ace-bioinformatics.org), so that any necessary steps can be taken to contain and rectify the result of the incident or misuse. Misuse of ACE HPC resources can lead to temporary or permanent disabling of accounts, and administrative sanctions or legal actions.

You are responsible for reporting, as soon as possible, any suspicious activity you notice on your account, and exposure or compromise of passwords. The notification email is support@ace-bioinformatics.org.

2.2.2.2 Data Protection and Confidentiality

You are responsible to ensure the confidentiality of any data that you use or store on the ACE HPC and ensure compliance with any legal or regulatory frameworks that govern those data. Such data may include: intellectual property such as research in progress; protected health information such as patient medical records; personally identifiable information such as data containing names or your country's National Identification Numbers, student registration numbers etc.; proprietary data, such as data owned by a specific company, or licensed applications. It is your responsibility to be aware of any requirements on a particular data set.

ACE HPC resources are operated as research systems and should only be used to process, store data related to authorized research. any addition encryption required by the data owners must be applied by the user if system level encryption is required for a project it must be included in the project request or as an amendment to an existing project request (for example, a backend database or an application that will hold sensitive data).

2.2.2.3 Acknowledgment

Papers, publications, and web pages of any material, whether copyrighted or not, based on or developed under ACE-supported projects must acknowledge this support by including the following statement:
"Portions of this research were conducted with high performance computing resources provided by the African Centres of Excellence in Bioinformatics and Data Intensive Sciences (https://ace.ac.ug) Said acknowledgment shall encompass the citation referencing the following ACE publication, which can be accessed at the following URL: https://doi.org/10.37191/Mapsci-JIDM-1(2)-006 may include the ACE logo when appropriate at the following URL https://drive.google.com/drive/folders/1tA8ptOv0hTbml0TbzXaIz9lw0Au4E1GC?usp=sharing

2.2.2.4 Software Licenses

All software used on HPC@ACE systems must be appropriately acquired and used according to the specified licensing. Possession, transmission or use of illegally acquired software on HPC resources is prohibited. Likewise, users shall not copy copyrighted software or materials, except as permitted by the owner or the copyright. Project requests should include the software that will be used and if there is a request for commercial software licenses this should be directed to the ACE Centre Director and the Operations team.

2.2.2.5 Final Reports

Requests for subsequent resource allocation awards will not be permitted until an end of project report has been received for all prior awards. It is recommended that continuing or ongoing projects also include a copy of prior award final reports as an attachment to the submitted resource request proposal.

2.2.2.6 Read the announcements

Users are responsible for reading the system messages and announcements. These will appear as messages during login, and will also be sent to all users at their registered email. It is the users' responsibility to monitor that email account for messages.

2.3 System Protection, Data Retention and Recovery

2.3.1 Backup and Retention

ACE-UHPCC provides daily backups of Home Directories for disaster recovery purposes only. Backups are retained for 90 days. Project directories are not automatically backed up. It's the responsibility of the project owner to ensure critical data is saved elsewhere.

Although ACE takes steps to ensure the integrity of stored data, ACE does not guarantee that data files are protected against destruction. HPC users are strongly encouraged to make backup copies of their data.

ACE reserves the right to remove any data after a user account is deleted or a user no longer has a business association with ACE.

2.4 Monitoring and Privacy

2.4.1 Privacy Policy

ACE HPC users have no explicit or implicit expectation of privacy. ACE retains the right to actively monitor all HPC resources, activities on ACE systems and networks and to access any file without prior knowledge or consent of HPC users, senders, or recipients.

2.4.2 Data collected

The ACE servers hold details of user accounts, thereby enabling a user to log in and use the resources of the ACE HPC. The following data are collected via either the account application process or service usage and held and maintained for each user:

- Name
- User identifier (account name)
- Institution affiliation
- Project affiliation
- Email address
- Contact telephone number
- User administration history
- Login history (session begin/end times and originating IP address)
- Resource consumption (in the form of job records accumulated by the job scheduler)
- Use of licensed applications (in the course of ensuring license term compliance)

These data are held on ACE system from the time the user's account is created, whether or not the user ever makes use of the ACE HPC. Unused accounts or accounts that remain idle for 6 months will be disabled. Reactivation requires the project owner or the ACE director to approve.

Research data held in home directories or other personal or group storage areas is stored, as required for the fulfilment of ACE services. This data is stored until purged by the user, or by the ACE HPC to enforce policy such as termination of account and expiry of access period (such as an account that has been disabled).

From time to time we may gather publication data from external journal or preprint listings in order to assess research outputs facilitated by ACE computational infrastructure.

2.5 User Problems and Staff Response

Users are welcomed and encouraged to send email to if they have problems or concerns relating to the HPC@ACE. The HPC staff will respond during normal weekday business hours.

2.6 Scheduled Maintenance

To improve system security and availability, a monthly maintenance cycle has been instituted. This cycle will generally involve a reboot of some nodes (not the entire cluster).
Unscheduled maintenance that requires a longer downtime will be announced separately to the ACE users email list. Every effort will be made to minimize disruptions.

2.7 Resource Scheduling and Jobs

The ACE HPC resources are shared by many users. The ACE uses a workload management system to implement and enforce policies that aim to provide each user with fair, but limited, access to the HPC clusters.
Jobs exceeding their allocated resource amounts will be terminated by the system or the system administrators with little or no warning. In order to avoid loss of data due to unexpected termination, users are strongly encouraged to checkpoint running jobs at regular intervals. Misuse of the system, deliberate or otherwise, is subject to the three strike policy.

2.8 General Storage Quotas

2.8.1 HPC User Home Directories

Default Quota: Each user is initially allocated 50 GB of storage.
Maximum Quota: Upon submitting a valid request and justification, a user's storage allocation can be increased up to a maximum of 200 GB.

2.8.2 Project Directories

Default Quota: Each project is initially allocated 1 TB of storage.
Maximum Quota: With a valid request and justification, a project's storage allocation can be increased up to a maximum of 5 TB.

2.8.3 Procedure for Requesting Additional Storage:

Submission: Users or projects that require storage beyond the default quota should formally submit a request to the HPC administration via [HPC admin email/contact].

Content of Request: The request should comprehensively detail:

- The justification for the additional storage requirement.
- Specifics of the project necessitating the increased quota.
- Estimated data sizes.
- The duration for which the additional storage is needed.

Review Process:
The HPC administration team will review the request. If the request is deemed appropriate at this initial level, it will be forwarded to the Center Director for final approval.
Notification: Users will be apprised of the final decision within [specified duration, e.g., "two weeks"].

2.8.4 Overage and Clean-up

Warning Notification: Users will be alerted when their storage consumption crosses the 90% threshold of their allocated quota.

Exceeding Quota:
If a user or project surpasses its designated storage quota, write access may be provisionally revoked.

Write privileges will be restored once the user or project team takes measures to reduce stored data to align with their assigned quota.

Temporary Storage Maintenance:
Data housed in temporary storage zones will be systematically deleted following 30 days of inactivity.

2.9 Account Expiration

The ACE audits cluster accounts annually, and all accounts not associated with a valid email address will be terminated. This is because it is essential for the ACE to be able to contact all account holders for security and communication purposes. Accounts expire after the duration specified at the time of issuance. Users who wish to continue access beyond the allocated duration, should apply to renew their access. Users are ultimately responsible for ensuring that all files are properly managed or removed prior to account expiration. Upon expiration, user accounts and associated data will be deleted.

2.10 Prohibited Conduct

The following provisions describe conduct prohibited under this policy and are subject to penalties:

- Unauthorized access to or use of ACE resources.
- Usage beyond the stated purposes in the allocation proposal.
- Unauthorized alteration of system configurations or disruption of IT administration.
- Unauthorized installation of software. Requests for software installations should be directed to support@ace-bioinformatics.org.
- Unauthorized access to others' accounts, files, or communications.
- Misrepresentation in electronic communication.
- Violation of copyright and software agreements.
- Interference with others' use of ACE resources.
- Commercial use or representation of unaffiliated groups without ACE authorization.
- Non-compliance with departmental or unit policies.
- Unauthorized facilitation of access to ACE resources.
- Unauthorized disclosure or exposure of sensitive/confidential information.
- Illegal, fraudulent, or malicious use of IT resources, including activities against Uganda regulations.
- Transmission of unsolicited bulk/marketing material.
- Harassment, threats, bullying, or promotion of hatred, terrorism, or illegal activities.
- Activity that degrades ACE HPC performance, deprives authorized access, or circumvents security unless authorized.
- Unauthorized use of security utilities or programs that exploit ACE HPC vulnerabilities.

Unauthorized personal benefit, political activity, advertising, fundraising, or actions prohibited by Uganda Law.

2.11 Penalties/Sanctions/Enforcement/Policy Violations

Breaches to this policy may result in a variety of penalties imposed. These include but are not limited to:

2.11.1 Account Suspension/Revocation

Accounts may be temporarily suspended or permanently revoked if compromised or abused. Your account may be suspended without advance notice if there is suspicion of account compromise, system compromise, or malicious or illegal activity.

2.11.2 Loss of Allocation

Unauthorized behaviour can result in loss of your current allocation, and may lead to the inability to obtain future allocations.

2.11.3 Administrative Action

Unauthorized activity may be reported to your PI, your supervisor, academic authorities, or ACE authorities for administrative review and action.

2.11.4 Civil Penalties

Civil remedies may be pursued to recoup costs incurred from unauthorized use of resources or incident response due to compromise or malicious activity.

2.11.5 Criminal Penalties

Activities in violation of university, national, or local law may be reported to the appropriate authorities for investigation and prosecution.

2.12 Exceptions

There are no exceptions to this policy. HPC users may not deviate from the terms of this ACE HPC Appropriate Use Policy in any way.

2.13 User Compliance Statement

I have read, understood, and agree to comply with the terms and conditions outlined in the ACE HPC policy. I acknowledge that it is my responsibility to use HPC resources in a manner consistent with the intended purpose and guidelines established by the organization. I understand that failure to adhere to these policies may result in disciplinary action, including the revocation of access privileges and other applicable consequences. By signing below, I affirm my commitment to uphold the security, integrity, and ethical use of HPC resources

Name ……………………………………….

Signature……………………………………. Date ………………………………………...

2.14 Approval

This policy is hereby approved and signed by

…… …………………………… Date: 10/11/2023

Daudi Jjingo ACE Uganda Centre Director

3 References

1. https://docs.hpc.cam.ac.uk/srcp/isms-docs/index.html
2. https://projects.ncsu.edu/hpc/About/AUP.php
3. https://hpcc.umd.edu/hpcc/policies.html
4. https://policies.umd.edu/policy/eab8c2d4-28d3-4eb9-96f9-69eb48daa334/
5. https://www.iiap.res.in/files/HPC%20Usage%20Policies.pdf
6. https://hpc.inl.gov/SitePages/Access%20and%20Usage%20Policy.aspx
7. https://www.nrel.gov/hpc/appropriate-use-policy.html
8. http://hpc.loni.org/users/hpcpolicy.php
9. https://research.computing.yale.edu/services/high-performance-computing/hpc-policies