ACCESS Acceptable Use Policy

v1.1
3/29/2023

Authors: Alex Withers, alexw1@illinois.edu

Approved by: Cybersecurity Governance Council, approved 8/30/2022

Table of Contents

Version Log

v1.0, 5/31/2022, Initial version, approved 8/30/2022 by CGC

v1.1, 3/29/2023, EC reviewed, awaiting EC approval.

1 Purpose, Scope, and Applicability

ACCESS and Resource Provider sites have legal and other obligations to protect shared resources as well as the intellectual property of users. Users share this responsibility by observing the rules of acceptable use that are outlined in this document.

When creating an ACCESS identity you must digitally acknowledge the ACCESS Acceptable Use Policy. Your on-line acceptance is your acknowledgment that you have read and understand your responsibilities as a user. If you have questions, please contact the ACCESS Help Desk at https://support.access-ci.org/open-a-ticket.

2 ACCESS Acceptable Use Policy

When you first create your ACCESS User Portal login and every 12 months thereafter, you will be asked to accept and re-acknowledge your responsibilities as an ACCESS user.

ACCESS and all affiliated Resource Providers have legal and other obligations to protect shared services and resources as well as the intellectual property of users. Users share this responsibility by observing the rules of acceptable use that are outlined in this document.

Your on-line assent to this Acceptable Use Policy is your acknowledgment that you have read and understand your responsibilities as a user of ACCESS services and any ACCESS Resource Provider resources, if applicable. If you have questions, please contact the ACCESS Help Desk.

By using ACCESS-managed services and/or Resource Provider resources associated with an ACCESS allocation (hereafter, "ACCESS services and allocated resources"), you agree to comply with the following conditions of use:

1. You will protect all accounts and access credentials (e.g., private keys, tokens & passwords) that you use to access ACCESS and ACCESS Resource Provider resources. This includes:
    a. Using a strong, unique password for your ACCESS User Portal account
    b. Only enter your ACCESS credentials into access-ci.org sites and ACCESS Resource Providers.
    c. Keeping your accounts and credentials private. You will not share your accounts nor access credentials with anyone else.
2. You will have only one ACCESS User Portal account and you will keep your profile information up-to-date. If multiple identities are discovered for the same individual, those accounts and profiles will be merged or voided at ACCESS's discretion.

3. You will not use ACCESS services or allocated resources for unauthorized financial gain or any unlawful purpose, nor attempt to breach or circumvent any ACCESS or Resource Provider administrative or security controls. You will comply with all applicable laws and relevant regulations, such as export control law or HIPAA.
4. You will immediately report any known or suspected security breach or misuse of ACCESS access credentials to the ACCESS Help Desk (https://support.access-ci.org/open-a-ticket).
5. Use of ACCESS services and allocated resources is at your own risk. There are no guarantees that resources and services will be available, that they will suit every purpose, nor that data will never be lost nor corrupted. You are responsible for backing up your data.
6. Logged information, including information provided by you 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 only as far as necessary to other organizations cooperating with ACCESS. You accept this necessary data sharing accordingly. See ACCESS Privacy Policy.
7. You must comply with ACCESS policies and those of ACCESS Resource Providers. Violations of either ACCESS or Resource Provider acceptable use and other policies may result in loss of access to both ACCESS services and Resource Provider resources. Activities in violation of any laws will be reported to the proper authorities for investigation and prosecution.
8. You agree to abide by the ACCESS Code of Conduct in your interactions with users and staff. See ACCESS Code of Conduct.
9. In manuscripts submitted for publication and any other citable works, you will acknowledge all ACCESS services and use of specific ACCESS Resource Provider resource(s) contributing to research results.
10. ACCESS uses Globus services for data transfer and other purposes. You accept the Globus Terms of Service (https://www.globus.org/legal/terms).

The following user responsibilities apply more specifically to Resource Provider-managed resources and services, including those allocated through ACCESS processes and any ancillary services to which access is authorized as part of an ACCESS-allocated project:

1. You will protect all access credentials (e.g., private keys, tokens & passwords) that are issued for your sole use by any ACCESS Resource Providers.
2. You will not allow any other person to use any of your ACCESS Resource Provider accounts and credentials.
3. You will only use ACCESS Resource Provider resources to perform work consistent with the stated allocation request goals and conditions of use as defined by your approved ACCESS project, this ACCESS Acceptable Use Policy, and the ACCESS Resource Provider's policies.
4. Access-granting organizations, your ACCESS allocation's Principal Investigator (PI), and ACCESS Resource Providers are entitled to regulate, suspend or terminate your access, and you will immediately comply with their instructions.

5. PIs are responsible for properly vetting users on their allocations and by doing so they are attesting that the ACCESS User Portal username belongs to the intended person. PIs will also ensure that users who have access to Resource Provider resources on the PI's ACCESS allocation adhere to this AUP.
6. Allocations on Resource Provider resources are awarded for open research intended for publication together with support for educational and training activities. You will respect all applicable intellectual property rights and observe confidentiality agreements.
7. You are responsible for working with your home institution and the relevant ACCESS Resource Providers utilized to determine what constraints may be placed on you by any relevant regulations such as export control law or HIPAA.