NCSA Acceptable Use Policy

Document Name: NCSA Acceptable Use Policy
Version: 1.0
Accountable: James Eyrich
Authors: Alex Withers

Reviewed: October 16, 2023
Approved by IIB Dec 15 2022

By using NCSA resources, you agree to abide by all University of Illinois and NCSA standards of conduct, and comply with the following conditions of use. For information regarding violations and enforcement, please refer to the NCSA Security Policies & Procedures.

1. You acknowledge having read the NCSA Security Policies and Procedures and complying with the NCSA Security Policies & Procedures where applicable.
2. This Acceptable Use Policy applies to users of NCSA resources, including users accessing resources with an external identity.
3. Resources are used in congruence with the University of Illinois Policy of Appropriate Use and any additional requirements set by sponsors.
4. All applicable laws, regulations, intellectual property rights and confidentiality agreements are respected
5. You will not attempt to elevate your access beyond what has been authorized nor coordinate with others to do so.
6. You will not use NCSA resources for illicit financial gain or any unlawful purpose, nor attempt to breach or circumvent any NCSA administrative or security controls.
7. In some cases, your account may be granted access to sensitive data (i.e. ePHI, CUI, ITAR). In those cases you must accept the responsibility for maintaining the confidentiality of that data. The following apply to those systems that process and store that data:
    a. I understand the account(s) assigned to me grants me access to information which may be sensitive, and I will reasonably safeguard all account access granted to me.
    b. You will comply with all applicable laws and regulations, working with the NCSA to determine what constraints may be placed on you by any relevant regulations such as ITAR, HIPAA, PII or Controlled Unclassified Information.
    c. You will not copy and/or move regulated or sensitive data without permission from the NCSA Security Office.
    d. I understand that I am not to use the access granted for any purpose other than for the performance of my official duties.
    e. I understand that I may not attempt to elevate my access beyond what I have been authorized nor coordinate with others to do so.
    f. I understand that friends and family may not have access to work-related accounts, credentials and files.
    g. I understand that my daily job responsibilities may involve viewing sensitive data and I accept the responsibility for protecting this information, regardless of my physical location, from unauthorized viewing and for protecting my account(s) from unauthorized access.
    h. I further understand that access granted to me to perform my duties may permit me access to information which is confidential and protected under State and Federal laws.
    i. I further understand that any sensitive information viewed while performing my job duties is not to be shared, discussed, or disseminated unless required to carry out my job-related duties.
    j. I will ensure that digital media and printed materials containing sensitive information are responsibly handled and stored, and subsequently securely destroyed when appropriate.
    k. I further agree to handle all data in accordance with my applicable University Information Security Policies (see also https://www.aits.uillinois.edu/reference_library/it_policies).
8. You will protect the access credentials (e.g., passwords, private keys, and/or tokens) issued to you or generated to access NCSA resources; these are issued to you for your sole use. Protecting these credentials includes the following requirements:
    a. You will have only one NCSA User Account.
    b. You will keep your profile information up-to-date.
    c. You must use a unique password for your NCSA User account.
    d. You must only enter your NCSA password into trusted resources.
    e. You must not share any of your NCSA credentials with any other person.
9. Suspected security breach or loss or misuse of NCSA access credentials are to be immediately reported to NCSA Help Desk (help@ncsa.illinois.edu or +1 217.244.0710) as per the NCSA Security Contact Process.
10. Relevant access-granting organizations, Principal Investigators (PIs) or sponsors, and the NCSA are entitled to regulate, suspend or terminate any access.
11. Use of resources and services through NCSA is at your own risk. Unless contractually agreed upon, there are no guarantees that resources and services will be available, that they will suit every purpose, or that data will never be lost or corrupted. Users are responsible for backing up critical data.
12. Logged information is used for administrative, operational, accounting, monitoring and security purposes.
13. Violations of NCSA or University policies can result in loss of access to resources and potentially include administrative actions. Violations of laws or destruction of property will be referred to appropriate governing agencies that may pursue criminal or civil prosecution.