NCSA Information Security Policy

Document Name: NCSA Information Security Policy
Version: 2.2
Accountable: James Eyrich
Authors: Adam Slagell, Alex Withers

Reviewed: August 22, 2023
Approved: August 24,2023 by IIB

Mission & Purpose

The National Center for Supercomputing Applications (NCSA) is an interdisciplinary hub at the University of Illinois at Urbana-Champaign, which serves the computational needs of the nation's scientists and engineers through the cyberinfrastructure (hardware, software, & services) they develop and support.

The NCSA Security Office supports the mission of the Center by assuring the confidentiality, integrity and availability of the Center's digital assets and resources and those of its partners. This is achieved through monitoring, incident response, proactive security design, education, and awareness activities at the Center and with its collaborators.

This policy document supports these missions by promoting sound practices for securing digital assets by educating the tenants of NCSA buildings and networks of their responsibilities and the procedures and processes at NCSA.

Scope

This policy is applicable to all University **workforce members & students** with any appointment at NCSA, **sponsored guests and vendors** allocated physical space in an NCSA building, and any person responsible for resources hosted on NCSA networks (referred to hereafter as "stakeholders"). It complements other NCSA and UIUC security policies. Links to these and other security policies can be found in the reference section of this document.

This policy does not cover building security, though it covers the physical protection of electronic devices that store University data.

Responsibility

As security is a process, and not a technology, security is everyone's responsibility and requires cooperation, awareness and ownership by all parties. Therefore, not only does the Security Office hold responsibilities for protecting NCSA assets, but so do all the stakeholders in our shared offices and on our networks.

Security Office Responsibilities

The Security Office is responsible for investigating and coordinating responses to security incidents as well as proactively monitoring NCSA networks and systems for indicators of compromise. Many of the services provided and maintained by the security team are for these purposes.

The Security Office provides assistance in the design and implementation of security architectures, assisting the resource providers at NCSA in developing systems that are hardened and more resilient to cyber attacks. This requires the security team to maintain leading edge skills in their domain and to translate that expertise to the other engineers and developers at NCSA.

The responsibility to uphold University and NCSA policies and agreements related to cyber security also falls on this office. They must therefore monitor and audit for compliance, and take actions (e.g., removing a system from the network or reporting violations to Human Resources and appropriate management) to support NCSA's obligations.

The Security Office must also ensure that NCSA systems are not used in an attack against itself or other institutions and will remove systems from the network as needed to do so.

Finally, they hold responsibility for providing adequate training, awareness and guidance to NCSA staff, partners and customers.

Stakeholder Responsibilities

Persons in NCSA buildings and on NCSA networks (i.e. NCSA stakeholders) have a responsibility to follow the security policies and procedures of NCSA, UIUC and the State of Illinois. That includes this policy, but also the applicable policies referenced at the end of this document. This list may not be exhaustive, as special agreements with vendors or project specific policies can have security implications as well.

Stakeholders are expected to cooperate with security, legal and regulatory investigations or audits. This includes being truthful, not exceding their authorizations, and never falsifying or destroying evidence.

It is the responsibility of all NCSA stakeholders to report security incidents or violations of these policies to the Security Office. Similarly, it is everyone's responsibility to promptly report a suspected compromise of their systems or credentials (e.g., passwords, security tokens, SSH keys, and digital certificates) so that abuse can be prevented as early as possible.

Finally, NCSA stakeholders must annually review this policy and sign off that they have done so. Security training will be provided at least annually as part of the Security Office's training and outreach activities. These are important not only to keep up-to-date with changing policies and procedures, but also with industry best practices and current security threats, which also change over time.

Policy

Privacy Expectations

The University and the NCSA respect the privacy of its staff and customers. However, both must both be aware that there are systems in place that actively monitor for indicators of compromise and record logs to support the IT infrastructure at NCSA. For example, NCSA monitors its networks in realtime for security and performance issues; shared systems record logs to a centralized log server; vulnerability scanners regularly scan systems and credentials for weaknesses; and security systems continuously monitor user interactions on shared systems looking for indicators of compromise, such as, execution of certain command sequences. These systems can therefore see all unencrypted traffic as well as laptop/workstation backups if encryption is not utilized.

In addition to this automated monitoring, manual investigations of security incidents or performance issues may require authorized staff to view traffic or files on NCSA networks and equipment.

As a state institution, stakeholders need to be aware that anything they do using University systems or for University purposes, is potentially open to FOIA requests. This includes emails saved on University systems, printed records, and things written on wikis or other forums at the University. As such, the University recommends that all employees have the following footer included on their University emails.

> *"Under the Illinois Freedom of Information Act (FOIA), any written communication to or from University employees regarding University business is a public record and may be subject to public disclosure."*

The privacy of others must also be respected, and unauthorized snooping of traffic or communications is a serious offense that will be reported to Human Resources (HR) or a guest's sponsor. This includes network traffic recording or any means of superseding ones authorizations to look at digital files they should not access.

Only the NCSA Public Affairs department or Director's Office has the authority to speak to the public about an ongoing security investigation. While the Security Office may share information with trusted partners or law enforcement to resolve an incident, they do not speak to the public about an ongoing incident. And even after the incident, they only do so while respecting the anonymity of individuals.

Appropriate use of NCSA Systems & Services

NCSA stakeholders are in a position of trust when given authentication credentials, such as, passwords, keys or tokens. These accounts are for their use only, and cannot be shared to give another party access to NCSA systems or resources. Furthermore, per the University's policies, passwords are high risk information and therefore cannot be stored or transmitted unencrypted. For example, NCSA passwords cannot be emailed unencrypted or put on a web site or wiki.

Stakeholders are expected to obey all relevant laws and regulations regarding computer "cracking", attacking, fraud, etc. Users of NCSA resources, including stakeholders, also agree not to attack NCSA systems or exceed their authority on them. This includes violating file permissions, impersonating others, stealing/cracking other users' credentials, and using NCSA systems as part of an attack on other computers or electronic equipment.

While the University respects academic freedom and has a broad mission, stakeholders need to take careful consideration of personal use of University owned systems or networks. For example, profiting or politicking with University equipment violates State law. Other activities may be legal but against the mission of the University. People are advised to contact the Ethics Office with specific questions about personal use of University equipment.

Operating Servers at NCSA

Reputational systems and services are run out of the Integrated Cyberinfrastructure (ICI) Directorate, which includes the Security Office. The ICI division leads meet regularly and with other stakeholders on the NCSA Internal Infrastructure Board to provide the best services possible for our workforce members, users and partners. However, there are many R&D projects that run their own internal services less formally. Regardless, operators of any service still have obligations and need to be aware of NCSA/UIUC policies and procedures.

Raised access floor (RAF) space is provided for servers at NCSA. Based on the needs of the project and costs, servers could be placed in either the main data center at NPCF or one of the smaller RAF spaces in the NCSA building. The Internal Infrastructure Board works with PIs (Principal Investigators) to find the appropriate space.

Running any service requires knowledge of and compliance with the NCSA Network Security Policy, which defines security requirements based on the network zone where the service is hosted. Servers are not to be run out of office or wireless networks, and server operators must subscribe to the NCSA Security blog to stay informed of current security issues.

Just as services provided by ICI must respect the privacy of users, so too must anyone else running services at NCSA respect user privacy, maintain transparency, and follow applicable laws. Failure to do this endangers NCSA's reputation and standing, and could result in a system or service being taken offline.

Finally, the Security Office must be involved early on when developing funding proposals that will place new infrastructure at NCSA. This is because special requirements could require extra planning by security staff or even have extra costs that must be accounted for in the proposal. For example, storing protected health information could require clearance with the University, contracts to be signed, and additional audits. It could also require offsite hot backups and special support commitments for emergency modes of operation, and all of this costs money and time.

NCSA Equipment Use

Many stakeholders have University laptops, workstations or other computer equipment assigned to them, for which they are responsible. This responsibility includes providing for the physical and cyber security of these devices.

For the cyber-protection of equipment, it is required that devices left unattended will lock within 5 minutes, requiring a password, passcode or biometric to access them. This is especially important of mobile devices, such as, tablets and laptops, but important for even workstations in shared offices or unsecured spaces. Even personal devices, if used for university business, must use such timed lockouts. For example, a mobile phone that is setup to use University email must have a passcode or biometric enabled.

Those who self-manage systems on NCSA networks are responsible for following security best practices and keeping their systems up-to-date. They must follow all University policies regarding anti-virus software, firewalls, and other security software. The Security Office will help keep stakeholders aware of these policies and best practices.

NCSA staff are usually allowed to take laptops and some other equipment home, but this must be done with approval from their manager and registration with Shipping & Receiving. They are responsible for inventory of NCSA equipment and must be informed of equipment that leaves the office or any transfers of equipment to other persons. Such equipment must still have a business purpose if taken home, and staff are again advised to contact the Ethics Office with specific questions about personal use of University equipment.

NCSA equipment that is lost or stolen must be reported to one's manager/sponsor and Shipping & Receiving. If it held high risk data as defined in University Policy, its loss must also be reported to the NCSA Security Office.

NCSA equipment with Blue inventory tags must be returned to Shipping & Receiving when no longer needed. It must not be disposed of personally, even if broken. From there, equipment will be securely wiped clean and either repurposed at NCSA, or sent to campus surplus.

Finally, personal equipment that is used on NCSA networks will still be monitored and must follow the NCSA Network Security Policy. Personal equipment must never be used to store high risk data for the University.

Data Security

The University has three categories in its Data Classification Policy: High Risk, Confidential, and Public. Stakeholders must follow University policies regarding these classifications and also inform the NCSA Security Office if they are in possession of any high risk data as this will require a data management plan.

University data that lives exclusively on a laptop, workstation or other device must be backed up regularly or moved to shared service that is backed up, like a wiki or file server. NCSA provides a backup service to all faculty and staff with an appointment and will help to configure its use on their systems.

Only University approved third-party cloud services are allowed for storing **unencrypted** high risk or confidential University data (this includes backups that may contain such data). If not pre-approved, data must be locally encrypted **before** being put on the third-party service.

Exit Process

Departing NCSA occupants and employees meet with the NCSA building manager who will collect any tagged equipment not transferred to another person as well as remove access to server rooms, which may house equipment with sensitive digital information.

NCSA accounts may or may not be deactivated, depending on the role the person maintains with the Center. However, if they are departing staff, they must be removed from all staff groups in NCSA authorization systems and staff email lists. They will also be removed from any other NCSA email lists unless the list owner actively approves of their continued membership.

Additionally, departing staff must acknowledge the NCSA Acceptable Use Policy, which includes a confidentiality agreement for workforce members with access to sensitive data, to ensure employees are reminded of their obligation to not discuss sensitive information after employment.

Security Controls

NCSA prescribes security controls consummate with the risk level of the information systems. Current controls are in place to prevent, detect, contain, respond to, and/or otherwise recover from security incidents. These controls are found in the following security policy documents:

- NCSA HIPAA Access Control Standard
- NCSA CUI Access Control Standard
- ACHE Facility Security Procedures
- Identity and Access Management Policy
- ACHE Vulnerability and Patch Management Standard
- NCSA Incident Response Policy
- NCSA Information Security Policy (this document)
- NCSA Network Security Policy
- NCSA Security Monitoring Policy

Systems or users may not bypass security controls either unintentionally or otherwise. The NCSA Security Office reserves the right to prevent such bypassing of security controls. Intentional bypassing of security controls may be treated as a violation of NCSA security policies.

Advanced Computational Health Enclave

The Advanced Computational Health Enclave (ACHE) is a special environment with restricted physical and electronic access at NCSA. Sensitive data including all electronic Protected Health Information (ePHI) and Controlled Unclassified Information (CUI) processed or stored at NCSA is done within this environment.

All NCSA workforce members who need access to this environment or who may come in contact with ePHI during day-to-day operations or an emergency are designated as a part of the NCSA Health Care Component (NHCC) of the University of Illinois Covered Entity. All NCSA workforce members who need access to this environment or who may come in contact with CUI during day-to-day operations or an emergency are designated as a part of *the NCSA Staff with ACHE Access* group.

All workforce members in the Covered Entity must take the official UofI HIPAA training annually, and all workforce members in *the NCSA Staff with ACHE Access* group must take CUI training. If they use laptops to access these systems, the devices must utilize full disk encryption. All laptops and workstations they use for this work must also employ password protected screen savers that automatically lock after a period of inactivity.

Removable media may not be brought into, connected to or used in the ACHE environment without explicit permission of the Security Office. If removable media is approved for use in the ACHE environment it must be encrypted in accordance with the BAA agreement and the Security Office. Currently this is AES currently employing 128 bit crypto key length.

The Security Office will verify compliance to the ACHE policy through various methods, including but not limited to, periodic physical inspection, video monitoring, security and business tool reports, internal and external audits.

Violations

The NCSA Security Office has the right and responsibility to take systems offline that are compromised (e.g. either attacking or causing harm to others). It also has the right and responsibility to take the systems offline of those persons violating NCSA security policies. In the event that systems are to be removed from the network in the case of security policy violations a ticket shall be created to track the incident. The CISO shall make the final decision and document this in the ticket, noting the impact on risk and thereby justifying the decision to remove the system. If the CISO is unable to be contacted and cannot make a decision in a timely manner, the ICI director will make the decision and document it in the ticket. While due effort is made to notify system owners before taking a host offline, this is not always possible in an emergency.

Depending upon the severity, type and recurrence of a violation, the Security Office may report the issue to supervisors, HR, senior management or even law enforcement. Violations of the NCSA or University's policies involving electronic Protected Health Information (ePHI) will be reported to the UofI HIPAA Privacy and Security Officer, and violators will be subject to disciplinary action as described by the University's policies.

Exceptions Process

There are exceptions and special cases to any policy. Requests for exceptions should be made to the Security Office and may be approved by either that office or the NCSA Director's Office. Note: the Security Office has a process to request exceptions. These requests are referred to as "variances" since they are requests to vary from NCSA's security policies.

Updates

This policy is reviewed annually by the Security Office. Feedback is solicited from the Internal Infrastructure Board for any recommended changes. New versions are approved by the NCSA Director's Office.

Questions

Questions regarding this policy or its implications can be sent to the Security Office (security@ncsa.illinois.edu) or the NCSA Help Desk (help@ncsa.illinois.edu).

References

University Security Policies & Standards

UIUC IT policies are posted at https://techservices.illinois.edu/office-cio/information-technology-policies

UIUC Security standards can be found at https://techservices.illinois.edu/security/illini-secure

The U of I HIPAA policy and resources page can be found at https://hipaa.uillinois.edu/

NCSA Security & Privacy Policies, Standards, & Procedures

Policies, standards, guidelines, and procedures developed by the NCSA Security Office are linked to from https://wiki.ncsa.illinois.edu/display/cybersec/Policies+and+Procedures

- NCSA Acceptable Use Policy
- Health Care Component Policies and Procedures
    - Risk Management Program for the Advanced Computational Health Enclave
    - ACHE Facility Security Procedures
    - ACHE Access Control Policy and Procedures
    - ACHE Vulnerability and Patch Management Standard
    - NCSA CUI Access Control Standard
- Data Retention Policy
- Identity and Access Management Policy
- NCSA Information Security Policy
- NCSA Physical Security Policy
- NCSA Security Contact Process
- NCSA Incident Response Policy
- NCSA Network Security Policy
- NCSA Security Operations Log Review Procedures
- NCSA Security Monitoring Policy
- NCSA Security Awareness Program
- NCSA Risk Assessment and Mitigation
- NCSA Risk Management Program
- NCSA Vulnerability Management Policy

Other Resources

1. University of Illinois Ethics Office (www.ethics.uillinois.edu)
2. Illinois Freedom of Information Act (www.uillinois.edu/foia)