NCSA Physical Security Policy

Document Name: NCSA Physical Security Policy
Version: 1.0
Accountable: Alex Withers
Authors: Alex Withers

Reviewed: June 23, 2021
Approved: Approved September 23, 2021 by IIB

Scope

This policy covers NCSA's Facilities: data centers and computer rooms. That includes the National Petascale Computing Facility (NPCF), 1725 S. Oak St., Champaign (NPCF), the NCSA 3rd floor data center in room 3003 at 1205 W. Clark St., Urbana. The ACHE compute cage in the NPCF and it's extension at NCSA in room 2105 is covered by the document but there are additional physical security policies documented in the ACHE policy and process documents.

This document applies to all NCSA Personnel, students, visitors, vendors and affiliates who would need access to the in-scope data centers and computer rooms.

Introduction

Physical access to computing resources can bypass many software, network, and other logical controls in place to protect those resources. This policy establishes physical security controls intended to mitigate physical security risks to NCSA's information assets.

For information regarding violations and enforcement, please refer to NCSA's Security Policies & Procedures located at:

https://wiki.ncsa.illinois.edu/display/cybersec/Policies+and+Procedures

Roles and Physical Access Coordination

- Physical access coordinator:
    - Tedra Tuttle, Assistant Director for Facilities, ttuttle@illinois.edu
    - Contact for coordination and physical access credentials. The physical access coordinator can provide a list of individuals with their current roles and permissions to authorized individuals.
- Facility manager:
    - Mohammad "Mo" Rantissi, Data Center Facilities Manager, rantissi@illinois.edu
- Physical security point of contact:
    - Alex Withers, Chief Information Security Officer, alexw1@illinios.edu
    - Maintainer of this policy and physical security controls and processes. Responsible for periodic audit and monitoring of controls and access lists.

Physical Access Controls - Facility Level

The required controls for physical protection are:

1. Limit physical access to systems, equipment, and the respective operating environments to authorized individuals.
2. Protect and monitor the physical facility and support infrastructure for systems.

3. Escort visitors.
4. Monitor facility activity.
5. Maintain audit logs of physical access.
6. Control and manage physical access devices (i.e. badges, identification cards).

Work areas not open to the public should be accessible by individual credentials using their iCards that can be revoked or changed for one user without impacting the others. This allows Facility Managers to promptly revoke or change access credentials when NCSA Personnel exit the project or credentials are lost or compromised, without concern that active participants may lose needed access. Access should be logged and access to those logs restricted to the Physical Security Point of Contact, Facility Manager and Physical Access Coordinator.

All access is obtained through the use of issued credentials (i.e. iCards). It is prohibited to gain access to any space without proper credentials. Every individual must use their own credentials and may not use credentials issued to another individual. All temporary issued credentials must be returned at the end of a visit.

Process for Granting and Revoking Physical Access

Any request for access (whether F&S, contractor/vendor, visitor, workforce member) must be documented as per the requirements in the Documentation section.

NCSA Personnel and students must have a request for access submitted to the Facilities Manager by their manager. The request must include proper justification. The request is approved by the Facilities Manager and access is granted.

For any type of work to be performed at the facility by Facilities and Services (F&S) and/or contractors/vendors requires a work authorization. The work authorization must be submitted two weeks in advance for approval to the Physical Access Coordinator and the Facilities Manager and the approved request is forwarded to the Physical Security Point of Contact. See the Documentation section for the work authorization request format.

Site access requires prior authorization and should be scheduled well in advance with the assigned workforce member sponsor. Sponsors are responsible for assuming that all requirements are met by the visitors for whom they are responsible. Site access will be only for the areas approved by the workforce member sponsor. Should access be needed to other areas, a new request is needed from and approved by the sponsor.

Non-NCSA Personnel visiting NCSA Facilities must be submitted to the Facilities Manager by the visitors sponsor who must be a workforce member. The request is approved by the Facilities Manager and access is granted. The approved request is forwarded to the Physical Security Point of Contact. These visitors must be escorted at all times.

Advanced Computing Healthcare Enclave

In addition to the procedures documented for general access, these areas have their own policies and procedures. Please refer to the NCSA ACHE Facility Security Procedures [3].

Revoking Access

Access to NCSA Facilities is revoked automatically when an NCSA workforce member leaves the institution or moves to another project precluding the need for access. Students, F&S personnel and contractors/vendors will have access revoked upon the end of their access granted term. Approval is granted for the following lengths of time:

- NCSA employees - granted annually and renewed as needed.
- Students - granted on a per semester basis.
- F&S - granted semi-annually and renewed as needed.
- Contractors/vendors- granted per work authorization start and end dates.

Other conditions for revoking access would include but are not limited to:

- Notification received by Facilities Manager of termination via employee exit form.
- When access credentials are submitted to the Facilities Manager.
- Emergency request is sent to the Facilities Manager or Physical Security Point of Contact to remove access.
- Audit findings determine unnecessary or unauthorized access.

Documentation

At times, these policies and procedures require documenting and authorizing activities. Unless otherwise noted, all requests, changes, etc. should be documented by NCSA. Details on the documentation will be detailed in a separate document.

Workforce member and student access request format:

- Start date:

- End date, if applicable
- Justification for access

The contractor/vendor or F&S work authorization request format:

- General Information
    - Title:
    - Contractor/vendor:
    - Subcontractor (if applicable):
    - Start Date and End Dates
    - Details
        - Location:
        - Description of work:
    - Potential for Service Impact:
    - Workers:
    - Supervisors:
    - Job Safety Analysis
        - Operation or Task Potential Hazards
    - Work authorization spreadsheet tracker with corresponding JIRA request ticket

Visitor request format:

- Requestor Name
    - Visitor info:
        - Name and Company
        - Justification for access
        - Where access is needed
        - State and End Dates

Auditing and Incidents

Physical access is audited annually by the Physical Security Point of Contact. The process for auditing physical access to NCSA facilities is documented separately with specific instructions ensuring that only authorized individuals have access and investigations and remediations are performed on unauthorized access. The process for auditing must cover: an audit of the physical access controls and a review of physical access privileges and activity.

The process for auditing physical access to the ACHE Cage and Room 2105 are documented by the Physical Security Point of Contact.

Physical security incidents shall be documented. Following an incident, any issues identified during the incident response process should be reviewed. Existing processes should be checked for accuracy and should be updated as necessary. It is recommended that a formal meeting occur to verbally review the incident to ensure that nothing was missed and all relevant information is recorded.

Monitoring

In addition to access logs, areas relevant to the physical security of highly vulnerable or valuable assets should be subject to video monitoring. Facility alarms should notify authorities in case of break-in, fire, or other conditions that require response from site protection.

Facilities and assets not normally manned should be monitored remotely and visited regularly to minimize the risk that damage (whether intentional or due to accident, weather, etc.) will go unnoticed.

Removable Storage Devices

The use of removable storage devices or external devices (e.g. USB Flash Drives) shall be restricted to NCSA Personnel only in order to safeguard and protect confidential data and information technology assets. Removable media containing sensitive data must be encrypted. Other authorized individuals may use removable media. Authorization for the use of removable storage devices must be granted in writing or by email by the physical security point of contact and specify the intended use of the device. The exception should be submitted as a ticket to the security group at help+security@ncsa.illinois.edu.

A list of authorized uses of removable storage should be maintained by the Physical Security Point of Contact and audited annually.

Disposal of Sensitive Documents, Media, and Equipment

Sensitive documents, media and equipment must be disposed of in a manner that protects the confidentiality of the information printed or stored.

- Shred documents containing sensitive information with a cross-cut shredder before disposal.
- Electronic media disks must be destroyed before disposing or repurposing as per University of Illinois policy [1] [2]. Secure destruction methods depend upon the type of storage media:
    - Magnetic media (e.g., backup tapes) must be purged prior to disposal, repurposing, or release;

- Disk drives must be purged prior to disposal or release; disk drives must be ***sanitized with a three pass overwrite*** prior to repurposing within the same unit or retiring;
    - Any media containing High Risk data that cannot be sanitized must be physically destroyed.
    - Exceptions must be approved by the Physical Security Point of Contact.
- Flash memory storage devices must be purged prior to disposal or release; flash memory storage devices must be ***sanitized with a one pass overwrite*** prior to repurposing within the same unit or retiring;
- Optical media (all types) cannot be reused and must be physically destroyed (e.g., physically shredded or incinerated); and
- NCSA will document actions associated with storage media disposal, if required by regulation. Restricted storage media disposal may be performed and documented by a university-approved storage media disposal service.
    - Some NCSA partners may require a certification of destruction. The physical security point of contact produces and stores these certificates.
- The Advanced Computing Healthcare Environment has additional procedures in addition to the requirements and procedures documented here. Please refer to the “NCSA ACHE Facility Security Procedures” [3].

Public Access, Delivery, and Loading Access

Access points such as delivery and loading areas, and other points where unauthorized individuals may enter the premises, should be controlled. This would include:

- limits on access to the delivery and loading areas, and other public access areas, to the degree consistent with required operations;
- inspection of incoming and outgoing materials, and separation of incoming and outgoing shipments, where possible; and
- isolation of these areas from information processing facilities and areas where information is stored, where possible.

Additionally, all ingress and egress points must enforce access rules (i.e. require proximity card readers and retina scanners). Ingress and egress points may not be unlocked, propped open or otherwise bypass physical security controls without prior written approval from the physical security point of contact.

Supporting Utilities

Because equipment and services are vulnerable to failures caused by outages of supporting infrastructure such as power and other utilities, the following measures will be taken to ensure the integrity of that infrastructure:

- Ensuring that supporting utilities are adequate to support normal operations of the systems
- Limiting physical access to utility supply lines, e.g., by ensuring that breaker boxes and HVAC control are in a locked location

- Making reasonable provision for redundant equipment and backups (e.g., a uninterruptible power supply, or UPS) in the event of supporting utility failure, at least for systems deemed critical
- Monitoring environmental factors such as power and temperature and triggering a shutdown of easily damaged systems when those factors exceed tolerances

Cabling Security

Telecommunications cabling carrying sensitive data or supporting information services should be protected from interception or damage. Network administrators should consider implementing logical controls that will act as countermeasures to man-in-the-middle and other attacks that may involve network cabling. However, the following physical controls should also be implemented:

- Physical access to cabling and network equipment should be limited and restricted to the extent feasible;
- Cables and equipment should be marked appropriately; and
- Maintenance on cabling and other physical network infrastructure should be documented.

Removal of Property to Off-premises Locations

Equipment, information, or software should not physically be taken off-premises without prior authorization (see section on documentation). When equipment, information, or software is removed from the premises, the following precautions should be taken:

- authorizations, removals, and returns of equipment should be thoroughly documented;

- the ACHE environment has special procedures for removal of property [3].

Exceptions

Any exceptions to this policy will require authorization from the physical security point of contact. The exception should be submitted as a ticket to the security group at help+security@ncsa.illinois.edu.

References

[1] Equipment Threshold Change - OBFS: https://www.obfs.uillinois.edu/equipment-management/equipment-threshold-change/

[2] Illinois Security Program IT15.2

https://cybersecurity.uillinois.edu/control

[3] ACHE Facility Security Procedures

https://wiki.ncsa.illinois.edu/display/cybersec/ACHE+Facility+Security+Procedures