NCSA Security Policies and Procedures

Updated June 26, 2009

Table of Contents

1. INTRODUCTION

This document establishes NCSA security policy and procedures. It provides methods for security policy development and implementation, assigns responsible management, and establishes procedures for security implementation and review, and resolution of security conflicts or incidents.

NCSA's computing and intellectual environment includes academic, government, and private sector researchers. The sensitivity of information and the openness of exchange are different in each of these environments. However, the history of NCSA shows the value of facilitating intellectual exchange and collaboration within and between these communities. NCSA's security policies and technical security architectures are designed to provide mechanisms whereby researchers can implement the level of security appropriate for their work.

NCSA's security strategy is to provide staff with tools and education concerning security policy and procedures, relying on individuals to use this knowledge and these tools to implement security measures appropriate to their work. In addition, centralized security measures and controls are implemented to assure basic security and to provide administrative review of security.

NCSA supports a variety of computing systems, services, and research projects for a diverse set of national and international academic, government, and private sector users. It is the responsibility of each participating user, staff person, or organization to use the tools available at NCSA to protect its assets and those of its staff and collaborators from injury, theft, or unauthorized use. Primary security concerns for NCSA include:

- Personal security of staff while working at any NCSA site including protection of personal possessions kept on site.

- Physical security of buildings, equipment, and records including protection from fire, theft, and unauthorized use.

- Protection of sensitive materials (see Definition of Terms). This includes compliance with non-disclosure and other security related agreements. Typically vendors or research partners provide information that they do not want distributed to others or used for purposes other than those stated in the agreement.

- Protection of the advanced computing and information infrastructure including the management of the computing systems and networks to prevent unauthorized use or denial of services, and to provide the protection of intellectual property (text, software, and data) stored or processed by those systems.

1.1. MISSION STATEMENT

The NCSA Security Policy and corresponding security standards, guidelines or procedure documents have been developed to provide reliable protection of various NCSA assets. These assets may be resources (computational systems, printers and copiers), information (e.g., intellectual property), infrastructure (e.g., networks and facilities), or relationships (e.g., agreements with private sector partners). Considered threats to these assets include—but are not limited to—direct cyber attacks from outsiders, improper resource use by employees and users, accidental disclosure of sensitive data, and natural disaster.

The NCSA Security Team's role is to (1) educate users on how to properly handle sensitive information and use their computers in a security conscientious manner; and (2) to support the central mission of the center by assuring confidentiality, integrity, and availability of its resources to its staff and researchers. In close collaboration with other NCSA groups, the Security Team helps protect our resources by focusing on assessing, detecting, and mitigating the risks to our network and computational systems. This policy document establishes a baseline of policies, as well as, standards and procedures that apply to all NCSA employees in order to meet these goals. Furthermore, it is the responsibility of the Security Team to maintain this document, update it and assist users in complying with it.

This policy and any corresponding documents are intended to be distributed to all NCSA employees, including full-time, part-time and student employees. This policy document itself is not sensitive, and its public disclosure would pose no threat to NCSA assets.

1.2. POLICY SCOPE

The NCSA Director's Office (DO) is ultimately responsible for establishing and implementing security. Any member of the Director's Office or any NCSA Division Director (DD) may be consulted concerning security policy and procedures for their respective division. Each DD is responsible for ensuring that the security policy and procedures are followed in their division.

This policy has been approved by the Director's Office and applies to all NCSA employees both current and future. This includes full-time, part-time, student and hourly employees. It does not include the vast user base of the NCSA's HPC resources, who fall under a separate user agreement. It applies to the use of any NCSA equipment and facilities, and personal equipment if attached to NCSA networks or storing NCSA intellectual property.

This policy does not replace the University of Illinois security policy, but is held in addition to it. NCSA is a department within the University of Illinois, and is thusly bound by all policies and procedures of the University. If there are any discrepancies between the University’s policies and NCSA’s, then the University’s takes precedence. However, where it is more restrictive, this policy takes precedence. Likewise, this policy does not necessarily address criminal or civil laws regarding the handling of special data (e.g., medical records) which may be more restrictive.

Furthermore, particular projects and partnerships at the NCSA may have additional security requirements. For example, the Blue Waters petascale computing project with IBM has additional confidentiality requirements derived from contractual agreements, and as such it has an additional security policy. Therefore, employees on that project may have additional rules to follow where that policy is more restrictive than the general NCSA policy.

While some computer systems require additional physical security protection mechanisms, this document is primarily aimed at information and cyber security. The NCSA Security Team is responsible for information and cyber security, and building security falls under the jurisdiction of the Administrative Office.

1.3. RELATED POLICIES

The University of Illinois Information Technology Policies[1] address some additional topics not covered in this NCSA policy and some of the same topics to greater detail. These policies also apply to NCSA employees as NCSA is a unit of the University. These topics include, but are not limited to:

- Software piracy, file-sharing and peer-2-peer utilities;
- Bandwidth usage;
- Handling of Personal Identifying Information; and
- Privacy policy and rights of individuals.

Refer to appendix 8.2 for URLs to additional University policies and manuals.

[1] http://www.cio.illinois.edu/policies/

2. AWARENESS

It is the policy of NCSA to provide an appropriate level of personal, physical and information security. Staff and others working at NCSA are required to read this document and take steps as needed to assure security. When security related questions arise they should be directed to one's supervisor, DD or the NCSA Security Officer.

Each staff member shall be provided with a copy of this NCSA Security Policy and Procedures document upon arrival to NCSA during the HR orientation process. It should be reviewed with his or her supervisor or DD during the first week of employment. The general policies and procedures as well as the detailed procedures for the person's particular division and work should be reviewed. The briefing should cover all the sections of this document. The new employee must acknowledge that they have read and understand the security policy, and this will be documented with a security acknowledgement form to be signed by the employee. A paper original form may be kept in the employee's folder in Human Resources (HR), otherwise an electronic acknowledgement by the employee will be stored in a database accessible by HR and the Security Team.

All new staff members are required to attend the first available new employee security training session. These sessions are held regularly, though a regular session may be postponed if there are only a few eligible attendees. Information on dates and times of sessions can be obtained from HR or the NCSA's Security Officer.

Each division should engage in a review of security policies and procedures pertaining to that division's activities at least once a year. Divisions will routinely monitor system and administrative activity related to security and the overall compliance of NCSA staff with security policies and procedures. Care will be taken to perform these reviews in an environment and manner that promotes contributions from the staff and makes them part of the effort of defining the procedures and proper levels of security. The DD will insure that these reviews are completed, and generate recommendations if needed.

Proprietary information will be clearly labeled (see section 6.4). Such outward, visible signs are useful in emphasizing to staff the importance of security in general. Staff are required to make use of this mechanism to maintain a sufficient level of awareness of security issues.

Supervisors will consider security procedure compliance when completing staff performance evaluations.

Security issues will be addressed with departing staff during exit interviews performed by HR (see section 6.3).

3. ASSURANCE

Defining and implementing appropriate security levels requires a continual process of confirming that both the defined policies and procedures are adequate for the ongoing work of the center, and that those policies and procedures are being properly communicated to and carried out by the staff and users. NCSA provides such assurances through a number of organizational and operational facets.

3.1. NCSA SECURITY TEAM

The NCSA computational security team, referred to just as the Security Team, helps to set guidelines and insure the integrity of the NCSA computer and network environment. They actively track and respond to security vulnerabilities and incidents. The Security Team also includes the Incident Response and Security Team, IRST (see Definitions of Terms).

3.2. STAFF RESPONSIBILITY

Each working area will have a DD as well as an individual staff member or members responsible for carrying out certain details of the policies and procedures for that area. It is the DD's responsibility to see that the detailed procedures section is maintained and followed in the daily activities of the staff in that area. The DD shall respond to requests for information from staff on specific procedures and interpretation of security policies.

It is the responsibility of each staff member to follow the procedures defined for an area in which he or she is engaged. It is also their responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in certain situations not specifically covered by the detailed procedures. However, in the latter case, a further responsibility exists to report the situation (described below) and have procedures clarified for future reference by other staff. Each staff member is expected to report any known or suspected violations of security procedures, or any exposure of known sensitive material to unauthorized personnel. This report should be made immediately to the NCSA IRST Team as identified in section 6.2 of this document.

Failure to comply with the policies and procedures within this document can result in disciplinary actions, up to and including termination, as per University and NCSA policy (see section 8.2).

4. NCSA FACILITIES PHYSICAL SECURITY

4.1. PHYSICAL SECURITY

This section of the NCSA security policy is concerned with physical security. All references to security in this section are related to physical security. Issues of electronic data security and intellectual property are covered elsewhere within this document. Physical security includes building and room security as well as physical security devices such as locks and physical restraints. Physical security is related to electronic data and intellectual property security. The ability to physically access a computer or paper files may compromise the security of electronic data. Physical security depends on many things. Building construction details such as the type of floors, walls, roof and especially windows are important. Windows that can be opened more than six inches are a security risk, especially at ground level.

Alarms and other security systems tend to increase building security. Some of the types of security systems in NCSA buildings are door monitor systems and after-hours motion detection and alarm systems.

The type, quantity and value of equipment and information located in NCSA buildings are important security factors. The more desirable or marketable these items are, the more likely it is that someone will attempt to breach NCSA security.

4.2. NCSA BUILDING SECURITY

As of September 2005, NCSA is located in two campus buildings (Advanced Computations Building, and NCSA Building) on the University of Illinois campus. The Petascale Computing Facility is under construction in 2009, which will eventually replace the Advanced Computations Building for our needs. The nature of these buildings directly affects NCSA physical security. Following are descriptions of the security systems, procedures and related issues for each building. Plans of all NCSA space indicating room usage and occupants are maintained and are available at request from the Director for Administration.

NCSA's normal business hours are from 8:00 a.m. – 5:00 p.m., Monday through Friday, except holidays. In general, visitors are not required to sign-in. All University buildings are cleaned by Building Service Workers (BSW) and maintained by trades people employed by Facilities and Services (F&S). All University buildings have space allocated to F&S for BSW's and mechanical systems.

4.2.1. Advanced Computations Building (ACB)

NCSA occupies all of ACB with the exception of space dedicated to mechanical systems and custodians. ACB entrances and computer rooms are to be locked at all times and use a keycard system to gain entry. Video cameras are located at all entrances and are monitored by staff in the control room. An intercom and remote lock release system is used at the main entrance to allow entry to authorized personnel who do not have keycard access. ACB is not open to the general public and is staffed 24/7/365.

4.2.2. NCSA Building

The NCSA Building is where most of the NCSA staff are located. North and south doors are open during regular work hours, and require key card access after hours. Side doors are locked and require key card access at all times. The NCSA Building also has surveillance cameras at all entrances.

4.3. Physical Security Requirements

All building exterior doors are to be kept locked at all times except where specific procedures have been established to leave a door unlocked. Doors shall be left unlocked or open only while a staff member is in a position to monitor access through the doorway. No one shall provide or allow unescorted access to any building or room to anyone who is not known to them to be a trusted staff member. Staff are encouraged to challenge in a non-offensive manner anyone in an NCSA building or room whom they do not know. Any person who is suspicious or cannot provide staff identification must be reported to either your supervisor, DD, or the University police. If you witness a building problem, such as a faulty lock or door, a propped open door, or something potentially dangerous, you must notify your building maintenance department, supervisor, or DD.

Individual workstations are subject to the physical security of the users' offices. Users must control physical access to their office and thus their computer. All rooms shall be kept locked unless a staff member is in the room or within sight of the room (in a position to monitor access to the room) or specific procedures have been established to allow the room to be left unlocked. Staff may choose not to lock a room for brief periods during regular working hours if the room does not contain sensitive materials (see below). However, staff are advised to lock all rooms any time no one is there to monitor access (if for no reason other than protecting personal items).

All computer rooms and telecommunications closets/rooms are to be kept closed and locked. Allocated systems, production servers (see Definition of Terms) and related equipment are located in designated computer rooms. These rooms are to be locked with controlled access.

Laboratories and training rooms containing concentrations of computers and other valuable and/or sensitive equipment are to be kept locked with access limited only to authorized staff. In cases where public access to NCSA computers is allowed, security is maintained with physical locks and logon restrictions.

Confidential and proprietary information may be kept and used in various offices and other rooms throughout NCSA. Because it is not possible to control who may access NCSA spaces during regular business hours, and even after hours, NCSA staff are advised to lock their offices whenever they are away.

Office and building keys are distributed to NCSA staff and affiliates based on the Keys and Keycards policy (see Key and Keycards policy). Keys are requested via a form by supervisors and approved by the DD. Master keys are generally given only to senior full time staff and require the approval of the Director for Administration. The security team will coordinate with the DD of Facilities to perform regular audits of personnel who are listed as having master keys.

Equipment in an employee's office is the responsibility of that employee. If any equipment is moved, broken, replaced, or upgraded the Shipping and Receiving department must be notified.

Staff who use NCSA equipment off-site are responsible for the physical security of that equipment. Any NCSA equipment taken off-site needs approval by a supervisor and an Off-Site Equipment Usage Authorization form needs to be filled out with Shipping and Receiving. This equipment is tracked through inventory control and audited annually by the Shipping and Receiving department.

If your NCSA-issued equipment becomes lost, immediately report this to inventory control via Email (shiprec@ncsa.uiuc.edu).

If your NCSA-issued equipment is stolen then a police report will need to be filled out. You can contact the University Police by calling 333-1216. If the item is valued over $300 then you will need to call 333-8911. An officer will need to come and take a report in person. Once the police report is filed, a copy will need to be sent to Shipping and Receiving so that it can be removed from inventory.

If your NCSA-issued equipment becomes damaged and needs repair, contact your supervisor.

Machines that are decommissioned (surplused/scrapped) are to be sent to the Shipping and Receiving department. Prior to these machines being decommissioned the hard drives will be wiped so that data is unrecoverable in accordance with the Illinois Data Security on State Computers Act. The procedures for wiping the disks will follow the Illinois Public Act 093-0306 and industry best practices.

Machines that are swapped internally between individuals or groups, which contain proprietary data (original or derived), will need to have the hard drive wiped. The same procedure as above will be utilized on these machines.

5. NETWORK AND SYSTEM SECURITY

Network security deals with concerns about the integrity and confidentiality of data traversing the network as well as the potential for security incidents (denial of service, unauthorized access, etc.) that occur over the network.

5.1. INTERNET ACCESS TO NCSA

NCSA's Internet connections provide high performance access to NCSA resources. Internet access is provided through a set of Internet routers which may be configured with a number of packet filters and other "firewall" mechanisms in order to prevent certain types of attacks from entering NCSA or originating from within NCSA. Detail on NCSA's filtering or firewall mechanisms are available from NCSA's networking group or security team.

5.2. NCSA INTERNAL NETWORK

NCSA operates a backbone network between its multiple buildings. All connections to the backbone network will have termination points within NCSA-secured network closets in each building.

With the exception of networking (routers, switches, etc.) and security equipment (monitors), no computing devices are to be directly connected to the backbone.

Only NCSA or University owned equipment, or equipment that is approved by a users direct supervisor, is allowed to be connected to the NCSA network. This includes personal laptops, PDAs and wireless access points.

Wireless access to NCSA's internal network is through NCSA's managed wireless access points. No other access points are allowed to be connected to the NCSA network without approval of an individual's supervisor or DD, and coordination with the supervisor of Network Engineering.

5.3. COMPUTER SYSTEM SECURITY

There are two types of computing security on which NCSA has focused. These are 1) operating system security and 2) user data security. While these two types may be seen as having distinct boundaries between the users' and NCSA staff's responsibilities, both NCSA and its user communities must work together to ensure a secure environment for all.

The operating system security goals are fivefold: to prevent access to the systems by unauthorized users, to prevent users with valid logins from unauthorized data access, to prevent unauthorized use of computing resources, to maintain system availability, and to prevent errors by those authorized to make system level changes.

The security for the operating system environment is shared by the system administration staff of NCSA for those systems that are centrally managed, NCSA staff and researchers who choose to manage their own systems, and the vendors of NCSA operating systems.

Administrators of all machines are required to keep their machines up to date with the most current patches to the operating systems. All unnecessary services should be disabled. System scans may be performed by the security team for vulnerabilities on all NCSA machines, and administrators may be notified to install specific patches to address vulnerabilities (see section 5.8).

Machines running production services (e.g. web, email, database, etc.) are required to be located in a machine room (see Definition of Terms).

Administrators running Windows machines are required to install and run the NCSA site licensed anti-virus package, or another licensed anti-virus package approved by the NCSA security team. These also need to be kept updated according to the vendor's recommendations.

Individuals may choose to maintain and provide the management of their own systems subject to the approval of their supervisor, but they accept full responsibility for the security of that system and any systems that may be compromised due to negligent security administration of that system. For student machines, it is the responsibility of their immediate supervisor to ensure they are maintained in a secure manner. Administrators of systems must also make themselves available to the NCSA security team at any time for security related incidents that involve systems they administer.

If a machine appears to have been compromised it may be taken off the network by the authority of the NCSA security team.

If you feel your electronic workplace (e.g. your account, or machine you manage) is compromised, or if you observe suspicious electronic behavior you are not sure about, immediately cease access to the system (but do not turn off the system) and contact NCSA Security. NCSA Security can be reached via the NCSA Help Desk (217) 244-0710 or <help@ncsa.uiuc.edu>.

The security of NCSA computing systems has been designed to enhance the collaborative effort of those scientists who choose to work in the NCSA intellectual environment. NCSA policy is that the user should make the decisions regarding data sharing and has provided tools and instruction to its users to enable them to do so. Users are encouraged to make every effort to secure their own data.

5.4. ACCOUNT SECURITY

All accounts on NCSA resources will be authorized by the NCSA allocation process before activation. For account management on self-managed systems, if a user has an account on an NCSA public resource then they are approved to be added to the local system. It is, however, the administrator's responsibility to make sure all accounts on the system(s) they manage are currently authorized by NCSA.

Accounts are for use by only the authorized individual and are not to be shared. Passwords and private keys should never be shared with anyone (this includes supervisors, coworkers, and spouses).

Users should maintain the secrecy of private keys associated with their accounts. Private keys may be used with programs like SSH, or PKI certificates. Long-lived private keys, need to be protected by secure passwords and stored in files readable only by the owner. Users should always enter secure passwords when prompted for a password to protect a long-lived private key and should not use blank or empty passwords. NCSA allows for passwordless short-lived private keys typically defined as lasting a week or less. If you suspect the secrecy of a private key associated with an NCSA account may have been compromised, contact NCSA's Security Team immediately as identified in section 6.2 of this document.

New user account information, along with default passwords, will be mailed to users and this document should be saved and secured for later reference. Instructions for users who have forgotten their password are contained in that document. Users should set a new password during the initial login. If a new password has not been chosen within thirty days of account creation, the account will be locked.

Users of self-managed systems also need to follow the above procedures.

NCSA security staff may audit password files in an attempt to detect insecure passwords.

Accounts on allocated systems are centrally managed through the Allocations process. This process also regularly verifies valid accounts and can report any discrepancies.

System administrator accounts are maintained with strict permissions. Access to these accounts are centrally managed and monitored frequently.

NCSA does not allow clear-text passwords (static passwords over an unencrypted channel) for remote access to any systems. Kerberos, SSH, or other secure methods must be used.

Staff accounts are no longer authorized upon departure of the employee. Mass storage (mss) access is available for four months after accounts are deactivated. These access times are enforced on all allocated and production systems unless requests are made to your supervisor and approved by the DO.

5.5. File System Security

All system files on allocated and production machines are protected from user modification and are checked on a regular basis for modifications. Privileged programs are monitored as well for use or for unauthorized changes.

Remotely accessible file systems (such as NFS and Windows sharing) may be exported only to systems located on NCSA managed networks, and systems are not allowed to mount file systems from machines outside NCSA managed networks. Exceptions to this must be approved by the NCSA Security Team which can be contacted via *security@ncsa.uiuc.edu*.

In the course of their duties, system or security administrators may need to access files or directories in order to fix problems. But this is not to be done any more than is needed to correct the problem.

5.6. Data Classification

There are three categories of data classification that require different levels of security. The three classes are:

- **Non-sensitive (Public)** — Information that may be freely disseminated.

- **Confidential** — Data that the owner feels should be protected to prevent unauthorized disclosure, but wouldn't expose NCSA to loss if disclosed.

- **Proprietary or Export Controlled (High Risk)** — Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data which is covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, EAR 99, ITAR, and certain client specified data, which may include: contracts, non-disclosure forms, software, documents, and graphics. Such materials may also include intangible assets such as concepts, text, derived data, and graphic information in any form. Payroll, personnel, and financial information are also in this class because of privacy requirements.

These classes are coordinated with the University's Data Classification Policy section of the Information Security Policy, though they use the alternate labels in parentheses (e.g., *Public* and *High Risk*):

http://www.fs.uiuc.edu/cam/cam/viii/viii-1.2.html

The handling procedures for these are addressed throughout this document.

5.7. Data Integrity (Backups)

Backups are performed periodically on all production and many desktop and laptop systems. These backups are done to ensure data integrity in the event of hardware failures. General scratch and temporary areas on the disks are not backed up since these data areas are very large and are considered as temporary storage space only. Duplicate backup tapes are stored in an alternate secure area at another NCSA facility. Backups are kept for 90 days and after that time the tapes may be recycled.

5.8. System Administration Security Monitoring

Computer systems security is a very complex issue. While certain tasks can be automated, the basic level of security must come from those administrators who, as part of their training and job responsibilities understand their respective systems. The number of administrators and the time spent on system security varies with each machine. When potential security problems arise the security team's approach is to gather as much data as possible regarding the security problem without compromising system or data security.

There are automated procedures that monitor log files and they may, at times, need to be monitored manually as well.

Security scans are done periodically on systems by the NCSA Security Team. These scans are done to assess vulnerabilities and other system exposures. Administrators will be notified of any problems, and recommendations of best security practices may be included. These scans will be kept for at least 6 months. The Security Team (*security@ncsa.uiuc.edu*) can be notified if there are any questions about the systems from which these scans are originating.

Host and network intrusion detection systems may be used by the security team to monitor and track intrusion attempts and compromises. In the event of an intrusion the security team may add additional monitoring for the period of time the system(s) are under investigation.

5.9. *Electronic Mail*

As a productivity tool, NCSA encourages the use of electronic mail (email). However, users access the Internet, including email, at their own risk. NCSA is not responsible for anything received, downloaded, or viewed by users via the Internet. Specifically, email may deliver unsolicited messages that contain offensive content or malicious software (computer viruses, worms, etc.).

NCSA cannot guarantee email will be private. Email can, depending on the technology, be forwarded, intercepted, printed, and stored by others. People other than the intended recipient may possibly access email. Email may be stored in backups in systems that may be retrievable after traditional paper letters would have been discarded or destroyed. Staff should be aware email is analogous to sending a postcard such that the content is not protected.

Users are prohibited from (1) having their NCSA email accessed (e.g., POP'ed) from another email service, and (2) forwarding their NCSA email to another service other than CITES Express Mail. Having other email services like Gmail access your NCSA account via POP or any other protocol is inherently insecure as it requires a third party to store your NCSA Kerberos password, and such password sharing is prohibited elsewhere in this policy for several reasons. While it may be convenient to forward your NCSA email to another provider such as Blackberry or Gmail, this results in a loss of control for the NCSA. For example, if a sensitive email containing proprietary information is accidentally sent unencrypted, we can no longer track or delete all copies of it. Furthermore, we have no control over the security mechanisms or privacy guarantees of third party email providers.

In the course of their duties, email administrators may need to look through users mailboxes in order to fix problems. But this is not to be done any more than is needed to correct the problem.

Email is scanned as it passes through the NCSA mail server for viruses, spam, or malicious software. Spam can be automatically tagged or blocked with this system if a user requests it. Requests for either of these can be directed to help@ncsa.uiuc.edu.

It is against NCSA policy for NCSA staff to email sensitive material (see Definition of Terms) without permission from the project lead or the owner of the sensitive information. However, the owner of the information may choose to email sensitive information at their own risk. Encryption techniques are encouraged for emails of a sensitive nature.

It is prohibited to knowingly pass along viruses, chain letters, hoaxes, or other unsolicited email.

5.10. *Internet Use*

Attempting to break into any computer system at anytime from any NCSA resource (e.g., computer or network) is strictly prohibited. Furthermore, releasing any worms or other malicious code on our internal network, or out on the Internet, is prohibited. The only exceptions are for situations approved by the NCSA Security Team (e.g., penetration testing), or research projects that are approved by a DD (e.g., approved security research projects with appropriate safeguards). Attempting to subvert or avoid any NCSA electronic security system, or to bypass any network-based security mechanism is similarly prohibited.

Intentionally obtaining, sharing, storing, viewing, emailing, or downloading items of an obscene or graphic nature including but not limited to, pornographic, sexist, racist, or illegal materials and/or any information/graphics that violate any of the policies of NCSA or the University is prohibited.

Using NCSA resources to advertise or sell commercial products and/or services is strictly prohibited. NCSA resources shall not be used for hosting Internet domains unaffiliated with NCSA related projects. The NCSA DO reserves the right to remove any content being served from its web servers—at any time—that it deems in appropriate or not inline with its mission and goals as an institution.

6. PROCEDURES

6.1. ESTABLISHING POLICIES AND PROCEDURES

Each DD responsible for a given area, requiring additional security policy and procedure definitions not covered herein, will be responsible for establishing these applicable specific security policies and procedures. In cases involving multiple NCSA divisions, the responsible DD's will work together or specify a responsible person to establish the additional security policies and procedures.

DD's will participate in internal and external security reviews or audits in order to analyze, justify and revise current policies and procedures as they apply to their divisions. DD's will establish a reporting line, as necessary, within their division which ensures that security is maintained in accordance with NCSA policies and procedures.

The Director's Office will be responsible for coordinating changes to security policy and procedures. A yearly assessment of the current policy and procedures document should be done to see if any changes are required. Requests for changes will be reviewed by the appropriate DD, who will report the feasibility and costs of the proposed changes. All changes in NCSA security policies and procedures will be approved by the DO. New policies and procedures will, in general, be assembled as a document that may be reviewed by the DO, as well as by the staff responsible for carrying out the specific procedures. New policies and procedures may be made part of this document at the discretion of the DO. NCSA staff and Private Sector Partners will be notified when changes are made to this document.

6.2. INCIDENT REPORTS REQUIRED

It is the responsibility of any staff member aware of a security incident (see Definition of Terms), to report it immediately to the NCSA Incident Response and Security Team (IRST). The IRST is reachable 24 hours a day through the HelpDesk (*help@ncsa.uiuc.edu*), or by phone at (217) 244-0710. IRST will then investigate the incident, notify affected parties (if needed), and recommend corrective actions.

6.3. EXCEPTIONS PROCESS

Realizing that we cannot predict all special circumstances that may arise, there may be valid exceptions (both temporary and permanent) to this policy in the future that we do not want to address by changing the policy as a whole. The process for requesting an exception to this policy is the same as the process for requesting a change to this document (Section 6.1), and the exception must be approved by both the DO and the Security Officer. The Security Officer will maintain a list of all currently valid exceptions.

6.4. SECURITY IMPLEMENTATION PLAN

The DD shall discuss security policy and procedures with supervisors in the division. The DD shall specify the steps to be taken by each supervisor. The DD and supervisors will review policies and procedures and raise concerns and issues for change and improvement to be taken to the appropriate DO contact. All security violations and non-compliance situations will be reported to the DO and the Security Officer. The DO and Security Officer will work to rectify these situations.

The following are specific actions and responsibilities.

- The DD should discuss security on a regular basis at meetings with supervisors and staff.

- Division-specific guidelines will be drawn up covering physical security and computational security activities where appropriate to that division.

- Supervisors will keep their staff aware and informed of policies and procedures, and be responsible for security within their own area.

- Supervisors will make themselves available to discuss the NCSA Security Policy and Procedures document with each new employee. Employees are required to read this document and address any questions pertaining to it with their supervisor. Supervisors should review with each new employee the security policies and address security issues specific their role and responsibilities. This procedure is to be documented through the use of an electronic security document acknowledgment form that will be electronically signed by the employee and then made available to HR.

- For staff working under non-disclosure agreements (NDA) the supervisor will work to help clarify the nature and purpose of these agreements. No one will be allowed to work on a collaborator project which requires a NDA unless a signed security document acknowledgement form, and a project-specific NDA, is on file with HR.

- HR staff will conduct an exit interview with a departing staff member prior to the staff member's final working day at NCSA. This interview will cover, among other things, keys and keycards that may need to be collected, and a review of the non-disclosure agreements in effect for that person (if any have been signed). A discussion of the personal effects of the staff member will be made to attempt to identify any proprietary materials that may be among them and guard against such material leaving NCSA with the person. An employee exit form will be filled out and filed with the HR department.

- Security training sessions for staff will be conducted on a regular basis.

- Staff members will make visitors aware of NCSA's security policy and procedures where appropriate. Visitors passes, keys or keycards that are distributed to visitors, will be collected upon their exit.

6.5. Project Security Procedures

This section describes the procedures and policies to be followed on projects involving proprietary or other sensitive data. The most common type of project of this nature is one with a Private Sector Partner involving proprietary information, but any collaboration may need this degree of protection and it is therefore available to any researcher. Herein the researcher, whether a Private Sector Partner or not, will be referred to as the "collaborator".

Projects are activities in which NCSA staff works with collaborators to develop and deliver materials. Projects may involve planning, data transfer, processing or archiving, software development, hardware development, and reporting, including documentation and audio/visual materials. The project may involve people from various divisions within NCSA or the University. The DD responsible for the project has overall coordination responsibility for the project. For projects involving a Private Sector Partner, a primary point of contact at the DD level will be responsible for tracking the project and in particular for overseeing issues related to proprietary information.

6.5.1. Planning

In cases where proprietary information may be discussed it shall be the responsibility of the collaborator to clearly identify all material that is considered proprietary. This should be documented in the contractual agreement (CA) (see Definition of Terms) between NCSA and the collaborator.

Any projects requiring NDA’s will require a CA with the collaborator so that the NDA’s can be tracked. The CA will list any personnel working on the project who are required to sign an NDA. A copy of the CA will, at minimum, be kept with the Principal Investigator (PI) of the project and the NCSA Security Officer. Copies of the NDA’s will, at minimum, be kept with the PI of the project.

The NCSA PI for the project will be responsible to ensure that all NCSA personnel involved have signed appropriate security related forms (i.e. NDA’s) and are aware of the security issues involved in the project. The PI will also make available upon request copies of any CA employees are working under, or any NDA an employee has signed.

No NCSA user should access proprietary information without signing the appropriate NDA and being listed on the CA with the owners of that data.

Security actions for planning include determining what security issues are for the project, and then proceeding with the following steps.

1. The project will be given a code name and/or number if requested by the collaborator. This code will be used throughout the project in internal and external communications and planning tools and documents to identify and track activities associated with it. No NCSA planning or archive documentation will include a textual name associated with the project that might reflect the specific or general field of study.

2. Project participants shall be listed in the CA. This validation list includes NCSA, collaborator, and any other personnel. It is to include all individuals who will be allowed access to proprietary project materials. It may only be amended by signed common agreement between the collaborator and the NCSA primary point of contact. The validation list must be amended if, during the project, people join or leave the project. Only persons included on the validation list may access sensitive materials in any form. All references to access limitations imply limiting access to those on the validation list.

3. Obtain from the collaborator a written statement which describes the security related aspects of the project and indicates what action are necessary to preserve security. Obtain non-disclosure or other security related forms to be signed and all project related materials that are considered proprietary. This statement should be included in the CA.

4. No work on a project will commence prior to obtaining signed CA’s and any related documents (i.e., NDA’s).

5. The PI and collaborator will address security issues included in the CA with the NCSA Security Officer.

6.5.2. Project Implementation

This involves access to collaborator concepts, documents, data (including software), and any hardware or other physical assets. Data may be analyzed and manipulated by a variety of software and hardware tools to create intermediate work and deliverable materials. Security issues may involve access to documents and data, as well as exposure to concepts/information. Visual display of data may involve computer monitor displays, and various media.

Requirements for initial data receipt, if any, will be documented in the NCSA Data Receipt Form. This form will specify the nature of the data (proprietary, confidential, etc.), how data is received, and any storage requirements.

NCSA procedures for data management and access begins when the data is transferred from a collaborator controlled area to an NCSA controlled area (see Definition of Terms). NCSA will follow procedures herein for data stored only on computer systems operated by NCSA. All computer directories, files, and temporary storage areas used to store proprietary materials during the project will be maintained so that access is limited to only those with authorization.

If proprietary data is received in physical form (e.g. CD's, tapes, etc.) it shall be labeled "PROPRIETARY" on the media itself (if not so already labeled). Electronic data will be labeled according to the requirements determined with the collaborator. Other labels are acceptable on a per project basis. For example, IBM prefers it use the term "IBM Confidential" for proprietary materials.

Periodic audits will be done on any projects that have proprietary data stored on NCSA resources. These audits will include reviewing the CA and all personnel who are requiring NDA's, personal access to data, and any other security requirements.

Collaborator data and research information must be protected during display and media recordings. All display and recording of proprietary material on film, video or other graphic media will be conducted in a manner so as to limit access.

All derived data is required to be handled as the original data received.

An amendment to the CA will need to be made, and signed, when work is going to extend past the CA's original deadline.

When the project is complete, the authorized collaborator representative will be responsible for the removal of sensitive material. NCSA will not retain any proprietary materials once the project is complete. If any proprietary material is discovered after the end of the project, it will be returned to the collaborator or destroyed. A NCSA Data Release Form will be filled out on conclusion of a project along with completing any exit forms for the project. The data release form will specify the methods of removal, or destruction, of data. Destruction of data will follow the industry best practices.

General system backups are performed to insure the integrity of the system and its data. Backups of sensitive project information may exist beyond the life of the project (see section 5.7).

6.6. Publication and Presentation

Publications and presentations are restricted to the obligations contained within the CA. There are specific publication and presentation policies addressed with PSP collaborators in section 7.2.5.

6.7. Copyrights and Releases

As a general guideline, other than periodic review of potentially proprietary materials and securing clearances, the NCSA staff will take no special security measures unless requested. It is up to the owner of information to request special measures and to specify appropriate restrictions on the dissemination of sensitive information. When such a request is made, it must be done in writing and appropriate signatures affixed.

Copyright will be confirmed with collaborators providing text or graphic materials before such materials are included in any NCSA releases of printed or electronic material. If necessary (i.e., if such materials are not owned by NCSA or do not reside within the public domain), written permission to reproduce any such materials will be secured from the copyright holder prior to any NCSA use.

Also refer to the “Copyright Policies and Issues” page from the University:

http://www.cio.illinois.edu/policies/copyright/index.html

6.8. Newsletters and Public Information and Technical Materials

Staff will verify that written material submitted for inclusion in newsletters and other materials is not proprietary by following the same procedures above. It is the responsibility of the collaborator to specify in writing to NCSA, or otherwise note during the pre-publication review process of the material, if proprietary information is mistakenly submitted for an article, press release, or other publication.

Staff will also follow these procedures:

- Illustrative material obtained from internal NCSA sources: Verification with NCSA staff will need to be done to resolve copyright issues before such material is included in publications.

- Background or illustrative material not owned by NCSA: The staff will confirm copyright information with the contributor before inclusion in any publication. The contributor will be required to sign a standard release form. If any materials are to be restricted from dissemination, the contributor will specify it on the release form. A copy of the form showing restrictions will be provided to all staff involved.

- Permission to copy: staff will ensure that we have permission to duplicate vendor documents.

6.9. Employee Exit Process

Several steps must be taken when an employee leaves to protect the security and intellectual property of the NCSA. Many of these steps will be done automatically when the manager fills out the **mandatory** exit form, an important procedure for all departing employees—full-time, part-time and student workers. These procedures are described below.

- All inventoried equipment must be transferred to other employees or surplused through Shipping & Receiving on or before their last day of employment. If the device has proprietary or confidential information on it, it must be wiped before being transferred to another employee. Shipping & Receiving must wipe **all** data before surplusing devices.

- Allocations will deactivate accounts—including the Kerberos principle—for the departing employee as soon as possible. However, the employee's files that are stored in a shared file system may reside in backups for up to 1 year. This would include files in AFS, MSS or messages on the email server.

  - The departing employee may still have some affiliation with the NCSA and need an account for research partnerships or other activities. In this case, they can get a sponsored guest account before they leave. However, the account name must be different. This forces system administrators to actively grant them access to any non public servers. Not changing the account name could inadvertently leave the former employee with access to several internal machines. This is a consequence of the decentralized manner in which servers and services are administered at the NCSA. This procedure would result in the email account for the old account being deactivated.

- Email accounts must be deactivated immediately following termination. Deactivating an email account means the user will no longer be able to login to NCSA's mail servers to check their email. However, while the former employee can no longer access the email system, the email administrator may provide an alias from their old NCSA address to a new email address upon request. In this manner, mail sent to the user's NCSA email address would be delivered to a non-NCSA account.

  - It is very important that a departing employee is promptly removed from any NCSA email lists. Exceptions can be requested by a manager on a per person per list basis. Furthermore, any lists administered by the former employee must either be terminated or transferred to another employee's control.

- Physical keys must be returned and key card access disabled on or before the last day of employment.

7. PRIVATE SECTOR PARTNER PROGRAM

7.1. PRIVATE SECTOR PROGRAM (PSP) PARTNER CONSIDERATIONS

The Private Sector Program Partners (PSP partners, or just partners) have specific security requirements due to the nature of their work and our interaction with them. Much of the research conducted with our partners is highly sensitive and could cause significant harm to the corporation's competitive position if it were to fall into the wrong hands. Additionally, much of the work done here with our partners represents a major investment, and loss of the data or alteration of the data could cause a financial loss. Any dealings with partners should reflect sensitivity to the security of their data.

7.2. PRIVATE SECTOR PROGRAM PARTNER PROCEDURES

7.2.1. Representation with NCSA Staff and with Partners

It is the responsibility of the AD of the Private Sector Program (PSP AD) to act as a liaison between the partners and the DO in regard to security matters. This includes representing partner needs and concerns to NCSA and representing NCSA policies and procedures to the partners. The PSP AD will work with all NCSA staff to clarify the nature and purpose of non-disclosure agreements with the corporations and maintain a file of blank copies of the approved nondisclosure document for each company. PI's of any staff signing non-disclosure agreements will receive copies of the agreements.

7.2.2. Partner Interactions

The PSP AD is responsible for coordinating interactions between the Private Sector Program Partners and NCSA. He/She is the principal point of contact for the partners when a security question or issue arises. This does not restrict partner access to other staff, particularly when timeliness is important and the PSP AD is unavailable. Coordination includes, but is not limited to, the following:

- Coordinate visits by partner security departments.
- Oversight of security provisions in any agreements.
- Briefing new partner on-site representative on specific NCSA/Private Sector Partner Program security policies and procedures.
- Notifying partners if changes in the security policy and procedures document impact partner projects or the handling of sensitive materials.
- Support investigations of any incidents.

7.2.3. Partner Office Space

There is a shared office space for Private Sector Program Partner use. On occasion PSP Partners may be assigned a designated office space at NCSA. The legal agreement with each of those partners clearly establishes that the partner controls access to their assigned office. Each member of the staff must respect the office as if it were an extension of the particular corporation's headquarters.

a. In the case of an emergency where there is immediate danger to people, property, and/or legal liability which may be the result of a natural disaster (e.g. flood), man-made (e.g. accidental fire), or illegal/malicious computer activity (e.g. a machine within the office space performing illegal/malicious activities), a mechanism will be established for NCSA staff to have emergency access to PSP Partner office space for the sole purpose of addressing the danger. This emergency access mechanism for NCSA staff will include attempting to reach designated Partner contacts for notification.

7.2.4. Specific Partner Requirements

Individual partners may request, through contract negotiations, special security safeguards for their office space, computational equipment, networks and/or proprietary information. It is the responsibility of the PSP AD to communicate any such requests and final agreement to the DO and the PI's involved in the process.

7.2.5. Publication and Presentation

NCSA and its employees have the right to publish or otherwise disclose the results of the research performed at NCSA, subject to the following conditions:

1. A copy of the proposed complete manuscript for publication or presentation materials for other public disclosure must be submitted to the Partner at least thirty (30) days prior to any submission for publication or public disclosure.

2. If the Partner determines that their proprietary information is disclosed in any manuscript or presentation materials, the Partner is required to notify the University in writing within thirty (30) days of its receipt. Upon notification, the University will have proprietary information deleted from the paper or presentation or have the publication canceled. Any revised manuscript or presentation materials must be resubmitted to the Partner for review. The Partner has the right to object on the basis of criteria specified above. If the Partner fails to respond within thirty (30) days after its receipt of the initial manuscript or presentation material or subsequent revision, the author(s) may proceed with publication or public disclosure.

3. If the Partner determines that potentially patentable subject matter is contained in any manuscript or presentation materials, the Partner must notify the University in writing within thirty (30) days of its receipt. Upon receipt of such notification, the University has agreed to delay enabling public disclosure of such patentable subject matter for a period not to exceed three (3) months from the date of receipt of the manuscript or presentation materials by Partner in order to file for statutory protection (the delay period may be extended for cause on a case-by-case basis with the University's concurrence). Alternatively, the author(s) shall have the option of revising the manuscript or presentation materials to avoid disclosure of the potentially patentable

subject matter. Any revised manuscript or presentation materials shall be resubmitted to Partner for review, and Partner shall continue to have the right to object on the basis of criteria specified above. Should the Partner fail to respond within thirty (30) days after its receipt of the initial manuscript or presentation material or subsequent revision thereof, the author(s) may proceed with publication or public disclosure without delay.

The PSP office will be responsible for preparing and submitting all requests, in writing, to the Partner. Primary authors will work with the PSP office to ensure that the proper submission process has been followed and that copies of all related correspondence are maintained on file. Where the primary author is not affiliated with the University, it is incumbent on the co-authors of manuscripts and presentation materials to assume responsibility for ensuring that the PSP office is included in the permissions process so that proper documentation is assured.

The PSP office will notify participants in Partner-related research of their publishing/presentation responsibilities on a regular basis.

7.2.6. Reporting of Accidental Disclosures

Should any staff become aware of an accidental disclosure of partner confidential or proprietary material, or any other security incident that could affect Partners (such as a machine compromise), a report must be made, immediately, to the Security Officer and the PSP AD. The PSP AD will be responsible for notifying the DO, who will be responsible for notifying the Office of the Vice Chancellor for Research (OVCR), who will be responsible for notifying the affected partner. This notification process will be done in a timely manner.

8. APPENDIX

8.1. Definition of Terms

PSP AD: Assistant Director of the Private Sector Program.

Allocated systems: Computer resources where peer reviewed allocations of computing resources are made to academic researchers. Accounting is run in order to track resource usage for each user. These are typically referred to as the production compute resources or supercomputing machines.

Collaborator: A researcher working on a project with NCSA. Collaborators include Private Sector Partners, academic partners and vendors. An NCSA employee may be an NCSA collaborator for the purposes of security.

Contractual Agreement: A formal agreement between NCSA and a collaborator. Examples of these would be Operational Agreements or a Memorandum of Understanding.

DD: Division Director. NCSA Division Directors are responsible for NCSA divisions consisting of multiple teams of staff reporting to supervisors.

DO: Director's Office. The DO consists of the Director, Executive Directors, Chief Science Officer, Chief Technology Officer, and several Division Directors.

Export Controlled: Technology or documentation that is available only to permanent residents of the United States or nationals from one of the following countries: Austria, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, or the United Kingdom.

IRST: Incident Response and Security Team. The NCSA IRST is lead by the NCSA security team, and includes operations staff, network administration, and systems administrators.

A machine room is a physical location that has controlled and limited access to administrators and staff. There are machine rooms located in most buildings NCSA occupies.

NCSA controlled area: Machine or other resource that is owned and managed by NCSA staff.

OVCR: Office of the Vice Chancellor for Research. The Vice Chancellor for Research is the senior campus officer with responsibility for advancing research at the University of Illinois at Urbana-Champaign.

PI: Principal Investigator. The PI is the project lead on work with collaborators.

PCF: The Petascale Computing Facility which houses the Blue Waters system.

Production system: These are resources that are centrally managed by NCSA and are supported 24x7x365. These machines include the email servers, web servers, file servers, and other critical infrastructure resources.

A security action is a procedure or set of procedures carried out to provide the desired level of security.

A security incident is any action or situation that violates documented procedures or which compromises, or has the potential to compromise, proprietary or otherwise sensitive information.

Sensitive materials are those things that have been identified as requiring protection (confidential, proprietary, or export controlled).

Staff includes: NCSA employees (paid or unpaid, including full-time, part-time, and students) or other individuals working on projects for or at NCSA.

User is anyone with an authorized account from NCSA Allocations to use NCSA resources.

A visitor is anyone who is present in an NCSA building or room who is not a staff member.

8.2. UNIVERSITY POLICY REFERENCES

University CIO Policy page:

http://www.cio.illinois.edu/policies/index.html

University Academic Staff Handbook

http://www.ahr.uiuc.edu/ahrhandbook/default.htm

Campus Policy and Procedure Manuals

http://www.fs.uiuc.edu/luci/