



NCCS Cyber Security Training

Version 1.3
07/29/09

INTRODUCTION

The National Center for Computational Sciences (NCCS) computing resources are provided to approved users for research purposes. All users must agree to abide by all security measures described in this document. Failure to comply with security procedures will result in termination of access to NCCS computing resources and possible legal actions.

SCOPE

The requirements outlined in this document apply to all individuals who have an NCCS account. It is your responsibility to ensure that all individuals have the proper need-to-know before allowing them access to the information on NCCS computing resources. This training will outline the main security concerns. Specific use policies are covered in the NCCS Computing Policies document, http://www.nccs.gov/wp-content/accounts/nccs_computing_policy.pdf.

PERSONAL USE

NCCS computing resources are for NCCS business use only. Installation or use of software for personal use is not allowed. Incidents of abuse will result in account termination.

Inappropriate uses include, but are not limited to

- Sexually oriented information
- Downloading, copying, or distributing copyrighted materials without prior permission from the owner
- Downloading or storing large files or utilizing streaming media for personal use (e.g., music files, graphic files, Internet radio, video streams, etc.)
- Advertising, soliciting, or selling

ACCESSING NCCS COMPUTING RESOURCES

Access to systems is provided via Secure Shell version 2 (sshv2). You will need to ensure that your ssh client supports keyboard-interactive authentication. The method of setting up this authentication varies from client to client, so you may need to contact your local administrator for assistance. Most new implementations support this authentication type, and many ssh clients are available on the web. Login sessions will be automatically terminated after a period of inactivity.

When you apply for an account, you will be mailed an RSA SecurID key fob. You will also be sent a request to complete identity verification. When your account is approved, your RSA SecurID fob will also be enabled. Please refer to <http://www.nccs.gov/user-support/general-support/access/> for more information setting your PIN, logging in, and general access information.

DO NOT share your PIN or key fob with anyone. Sharing of accounts will result in termination. If your SecurID key fob is stolen or misplaced, contact the NCCS immediately and report the missing key fob. Upon termination of your account access, return the key fob to the NCCS in person or via mail.



DATA MANAGEMENT

The NCCS uses a standard file system structure to assist users with data organization on the systems. Below is a brief introduction to the most common file systems all users should be familiar with. More information about all the NCCS File Systems is found at <http://www.nccs.gov/user-support/general-support/file-systems/>.

Home

All users are given a home directory to store frequently used items such as source code, binaries, and scripts. This home area is shared between all systems. Since it is not local to the High Performance Computing (HPC) systems and it is very limited in size, users should not run batch jobs that perform large amounts of I/O in their home directory. Please see <http://www.nccs.gov/user-support/general-support/file-systems/home-directories/> for more information about home directories.

Project Directories

Each project is provided a directory to share common project files. Data such as source code, binaries, and scripts may be stored in this directory. Project directories are located in an NFS that is accessible from all NCCS resources as /ccs/proj. Please see <http://www.nccs.gov/user-support/general-support/file-systems/project-directories/> for more information about project directories.

Work Directories

Work space is available on each NCCS HPC system for temporary files and staging large files. This file system is much larger than the home directory. User jobs should perform their I/O to this file system. Additional details about work directories are found at <http://www.nccs.gov/user-support/general-support/file-systems/work-directories/>.

High Performance Storage System (HPSS)

The HPSS provides archival storage for NCCS users. The HSI utility allows automatic authentication and provides a user-friendly command line and interactive interface to HPSS. HSI should be used to transfer data to and from the NCCS HPSS. Please refer to <http://www.nccs.gov/computing-resources/hpss/use/> for more information.

Sensitive Data

Additional file systems and file protections may be employed for sensitive data. If you are a user on a project producing sensitive data, further instructions will be given by the NCCS. The following guidelines apply to sensitive data:

- Only store sensitive data in designated locations. Do not store sensitive data in your home directory.
- Never allow access to your sensitive data to anyone outside of your group.
- Transfer of sensitive data must be through the use encrypted methods (scp, sftp, etc.).
- All sensitive data must be removed from all NCCS resources when your project has concluded.

DATA TRANSFER

The NCCS offers two dedicated data transfer nodes to users. The nodes have been tuned specifically for wide area data transfers, and also perform well on the local area. There are also several utilities that the NCCS recommends for data transfer. Please refer to <http://www.nccs.gov/user-support/general-support/data-transfer/> for information about data transfer nodes and utilities..