Rules of Use for Sensitive Data

Version 3.2
3/12/2010

INTRODUCTION

The Oak Ridge Leadership Computing Facility (OLCF) computing resources are provided to approved users for research purposes including fundamental research, proprietary research, and research that is export controlled. All users must agree to abide by all security measures described in this document when performing any work on OLCF resources that is not fundamental research and/or publicly available information. Failure to follow the security procedures in this document may place sensitive data at risk and may have legal implications.

SCOPE

The term "sensitive data" includes any source code, object code, or data which is considered proprietary, intellectual property, or an area identified by a U.S. government agency as export controlled.

The requirements outlined in this document apply to all individuals processing sensitive data or running sensitive codes on OLCF resources. It is the information owner's responsibility to ensure that all individuals requesting access to sensitive data have the proper authorization before allowing them such access. This document will outline the main security responsibilities of users processing sensitive codes and data.

Please follow the guidelines in this document to ensure everything possible is being done to protect your data's confidentiality. Any questions or concerns regarding the security of sensitive data should immediately be directed to help@nccs.gov in a sanitized email containing no sensitive information.

GENERAL AND ADMINISTRATIVE

1. Users agree to the conditions of use set forth in the DOE Warning banner "Notice to Users":

   NOTICE TO USERS

   > This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

2. Users must ensure that only individuals with the proper authorization for sensitive information will have access to that information.
3. Security anomalies or concerns must be reported immediately to OLCF staff.
4. User actions are subject to monitoring, recording, and auditing.
5. Users will not attempt to test security mechanisms or to assume privileged roles.
6. Users will not share passwords or SecurID FOBS.
7. Fob PINs must be secured and protected in a locked container if written down.

SENSITIVE DATA TRANSFER TO/FROM RESOURCES

The OLCF provides secure copy (scp) and secure ftp (sftp) for the encrypted transfer of sensitive data. All sensitive data should be encrypted during transit to prevent unauthorized interception. Additionally,

users must transfer sensitive data directly to storage specifically assigned to each project for storing sensitive data. Users are not allowed to transfer sensitive data into home directories located under (/ccs/home/<username>).

A man-in-the-middle attack can defeat the protections provided by encryption and one-time-passwords by allowing an attacker to act as a proxy between OLCF resources and your client computer. Please take Secure Sockets Layer (SSL) certificate mismatches seriously as this could be a sign of a man-in-the-middle attack. If the ssh, scp, or sftp client you are using notifies you of changed keys please **do not authenticate.** For example:

> @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
> IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
> Someone could be eavesdropping on you right now (man-in-the-middle attack)!

In this event, send a request to help@nccs.gov with a request to verify the ssh fingerprint of the destination system. The current fingerprints of OLCF resources are available on the home page under the "User Support"->"General Support"->"Access" link http://www.nccs.gov/user-support/access/.

SENSITIVE DATA PROCESSING

The OLCF provides computing resources to fundamental research projects as well as sensitive projects. Users processing sensitive data must use only those computing resources specifically authorized for their project. The resources provided are shared resources, meaning projects from both sensitivity designations may concurrently run on OLCF resources. It is possible for foreign nationals to be on the information system while your code is running. The OLCF computing systems are configured to restrict the access to segments of the computing resources each user is using.

If your project requires dedicated access to OLCF computing resources, please contact help@nccs.gov to establish a reservation, otherwise you will be executing jobs on a shared resource. NOTE: Your project allocation will be decremented for the full usage of the computing system for the duration of the reservation.

DATA STORAGE

Non-sensitive Data Storage

Home (/ccs/home/<username>)

Users may store **only non-sensitive data** in their home directories. Users should **never store sensitive data** in this directory. This directory is a networked file system which may be accessed from all systems within the OLCF network, unlike your project space which is only available from systems authorized for processing sensitive data. Users should only store non-sensitive data in this directory.

Sensitive Data Storage

Project Space (/proj/<project ID>) **(This is not backed up)**

A specific project storage space is defined for each project with sensitive data separate from the users Home area and Scratch space. This project space is protected with strict access permissions; no world-readable data is allowed in this space. This file system should be used to store any sensitive code or data that is to be shared with authorized members on your project team.

Scratch (/tmp/work/<username>)

Users can store sensitive data in the scratch space provided locally to the system on which they are processing sensitive data provided that no world permissions (world-read, world-write, or world-execute) are enabled on the data or code stored in this area. The default permissions on this directory are owner access only (unix permission "700") as configured at the time of account creation.

One Bethel Valley Road
P.O. Box 2008, MS 6008
Oak Ridge, TN 37831-6008
E-mail: help@nccs.gov
Phone: 865-241-6536
Fax: 865-241-4011

Users should never change permissions or permission masks that would allow world-read, world-write, or world-execute access to any files in scratch storage.

The default lifetime of data in scratch storage is 14 days. Data may be removed from the scratch file system automatically after this period of inactivity.

High Performance Storage System (HPSS)

Users should **not** store sensitive data in HPSS for long-term storage. Users should never change permissions or permission masks that would allow world permissions to be enabled (world-read, world-write, or world-execute).

DATA VISUALIZATION

User should not display sensitive data on the OLCF visualization facility (EVEREST) unless only people approved for that data are within the EVEREST facility. If a user requires access to the EVEREST facility, they must contact help@nccs.gov and schedule a reservation for EVEREST.

DATA DESTRUCTION

When sensitive data is no longer required, users must purge sensitive data from OLCF computing resources within 30 days. This reduces the risk of data confidentiality being compromised.

All sensitive data must be removed from OLCF computing resources by using an OLCF approved secure deletion application. For non-archival storage resources, BCWipe has been approved for the secure deletion of sensitive data on our resources. BCWipe will securely overwrite the information contained in a file or directory with patterns of data as well as random data. The command 'bcwipe' may be used on all data in project and scratch space.

Sensitive data stored in HPSS should be deleted using the HPSS 'rm' command.

However, secure deletion of data in HPSS is impossible due to the hierarchy of disks, tapes, movers, and servers involved. To mitigate the risk associated with not being able to securely delete information from HPSS, all tapes, disks, and servers associated with HPSS are in locked cabinets with access restricted to authorized personnel. A degaussing procedure is followed for all tapes and disks removed from the HPSS system.

One Bethel Valley Road
P.O. Box 2008, MS 6008
Oak Ridge, TN 37831-6008
E-mail: help@nccs.gov
Phone: 865-241-6536
Fax: 865-241-4011

Sensitive Data Rules of Use: Signature and Authorization

I agree to follow these rules in my use of the OLCF resources. I understand that violations may be reported to OLCF staff and that I may as a result be denied further access to the resources.

Please sign and fax the completed document to (865)241-4011 or email to accounts@ccs.ornl.gov.

Affiliation: _____

Date: _____

Print Name: _____

Signature: _____

---------- **Internal use, do not write below this line.** ----------

The above named person is validated / revalidated to use the resources for one year from the date of my signature.

Affiliation: _____

Date: _____

Print Name: _____

Signature: _____

One Bethel Valley Road
P.O. Box 2008, MS 6008
Oak Ridge, TN 37831-6008

E-mail: help@nccs.gov
Phone: 865-241-6536
Fax: 865-241-4011