CERI COMPUTING POLICY (March 2, 2017)

General Information

Detailed information on the CERI computer network is available at http://www.ceri.memphis.edu/people/mwithers/CERIComputing

UofM Data Security Policy

The University of Memphis Policy UM1691 (http://policies.memphis.edu/UM1691.htm) governs the use, control, and access to restricted data. The definition of restricted data is broadly defined and includes that protected by the Family Educational Rights and Privacy ACT (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach Bliley Act (GLBA). In particular faculty, staff, and students should treat personally identifiable information and student grades and information as restricted.

Basic compliance with the policy will generally be met by loading all data directly into Banner via an encrypted connection and not downloading any data from banner, and by working with a University supported and maintained computer with all recommended OS updates and patches and with all recommended antivirus and anti-spyware software and updates. Also required is a strong password that is not shared with anyone.

Faculty are particularly encouraged to note that storing student grades on a local computer is illegal unless the files are encrypted (and the above requirements are met).

UofM Password Policy

The University Password Policy (available at http://www.memphis.edu/its/security/password.php) applies to all accounts at CERI. Passwords should be at least 12 characters and changed every 6 months.

Passwords and logins may not be shared.

User Accounts

Account Eligibility

All CERI faculty, staff, and students are eligible for computer accounts on both the Solaris and PC domains. Additionally, faculty and staff may request accounts for collaborators and guests.

Login Security

The first lines of security are user passwords. Users should follow the University password policy above. The University UUID password should **not** be used on local CERI Computers (e.g. Macs or Unix). Rather new passwords following the same UofM guidelines should be generated for use on local CERI computers.

Connections to CERI computers from outside the domain are restricted and ssh is used exclusively. Users requiring outside access should request such access by providing computing staff with services required and ip addresses prior to leaving.

Users should refrain from remaining logged in when leaving the immediate area of the console. Users with dedicated machines should lock the screen and users of public machines will be logged out.

Intended Use

CERI computing facilities are providing only in support of the missions of the University of Memphis, CERI and CERI partners.

The University Acceptable Use Policy is
https://umwa.memphis.edu/umpolicies/UM1535.htm

Expiration/Deactivation/Revocation

Under normal circumstances, user accounts will be deactivated 3 months after leaving CERI. User files will be deleted 3 months after that. In some cases, at the discretion of the computing staff, accounts may be disabled immediately and without notice if a security risk or inappropriate use is detected or suspected. It is the responsibility of a user's sponsor to transfer appropriate data files prior to deactivation of a user's account.

Sponsors

All computing accounts at CERI have sponsors which are in most cases the individuals supervisor or academic advisor. The sponsor is responsible for transferring appropriate data files prior to deactivation of a users account. The sponsor also requests creation of accounts and provides appropriate information for account creation. In the event that problems arise with a particular account and the user is unavailable, the sponsor is considered the owner.

General Conduct

Computing facilities should be considered a tool for conducting CERI and University of Memphis business. As such, personnel should conduct themselves following the same guidelines as set forth in CERI and University policy manuals.

Resources and Services

Disk, Memory, and CPU: Each user is restricted to a disk quota on servers. Requests for increasing quotas should be justified by the sponsor. Users should be considerate of others when consuming memory and cpu resources and restrict resource intensive activities to off-hours.

Software: Standard software packages are provided for general CERI use. Additional packages may be requested and will be considered based on cost to the center in capital and maintenance, general usefulness to the CERI community, and meeting the mission of the center.

Mail

- Large attachments and user lists should be avoided.
- Mail services are provided through the University postoffice system.

- Avoid spam.
- Remember that email is not necessarily private.

Printing

Printers are provided in each CERI house. Printing is not cost-free either to CERI or the environment and users should avoid printing large or numerous files unless necessary. Strive for a paper-free workplace.

Network

Access to the CERI computing network is entirely at the discretion of the CERI and University computing staff. Immediate removal from the network may result if security or behavioral violations are suspected.

Goal of Backups

The purpose of backup plans is to provide recovery from hardware, software, and system failures. Users are discouraged from using backups as a means of recovering deleted files.

Unfortunately, current resources permit backup of servers only. Desktop backups are the responsibility of the custodian.

Digital Storage

It is the intent of CERI to provide networked data storage for normal research and academic functions of the center. Requests for project space beyond the limitations of home directories and existing areas should be made to the computer committee. Projects that require substantial storage beyond the norm (e.g. greater than 1TB) should budget for additional storage. Owners of data are responsible for backups and long term archiving.

Support

Office Hours and Availability: Office hours will vary but support staff will attempt to provide assistance during normal University hours.

Administrative and root privileges of supported systems are reserved for computing staff only.

While installing an unsupported system is counter to the goal of providing a fully networked computing environment, those who choose to do so must conform to the following:

- No computing staff support;
- No NFS or other remote disk mounts;
- Do not participate in LDAP or similar authentication schemes.