User Guidelines for Securing Shared Computing Resources	Guidelines No.	ITS-1032-G	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	3-18-15	Revised:	
				Page 1 of 11

Table of Contents

1 Purpose

The ability to inexpensively and easily use computers and other technology devices has resulted in University departments promoting the sharing of technology resources throughout their organization. The technology that makes shared computing resources cost-effective and easily implemented also makes them a security risk. Shared computing resources need to be safeguarded to protect the privacy, integrity and availability of the data being stored and transmitted over networks. For that reason, security is a critical component in a computing environment in which resources are shared.

This document outlines the University's guidelines for sharing computing resources. Through the practices outlined in this document, University resources can be protected to minimize the risk of unauthorized exposure or modification of information, to aid in ensuring the availability of those resources and to protect each user from interference by another user or by the system itself.

This guideline applies to all University computing resources that are shared. This includes, but is not limited to, computers, laptops, workstations and any associated peripherals (e.g., copiers, printers, scanners, faxes, electronic storage media, etc.) whether used for administration, research, teaching or other purposes that are owned, leased, operated or provided by the University.

2 Entities Affected by This Guideline

Any user who connects to shared resources or processes and stores shared information is responsible for the security of the shared resource devices and data.

If shared directories are created, departments are responsible for their creation and for granting appropriate permissions for authorized users of the equipment.

Department administrators are responsible for ensuring that all shared computing resources meet CSU and University policies, standards and guidelines and that proper departmental information security practices are followed when the department implements the use of shared resources, including the protection of proprietary information and protected data. If needed, departments may apply more stringent security settings than stated in this document.
Information Technology Consultants, IT support staff, department employees, student assistants, graduate assistants and/or third-party vendors are responsible for ensuring that all computing resources that provide shared resources meet CSU and University policies, standards and guidelines and for assisting end-users in the appropriate tools and safeguards for sharing resources.

3 Definitions

a) Authentication: The process of confirming that a known individual is correctly associated with a given electronic credential (e.g., by use of passwords to confirm correct association with a user or account name). It is a term that is also used to verify the identity of network nodes, programs or messages.

b) Authorized: The process of determining whether or not an identified individual or class has been granted access rights to an information resource, and determining what type of access is allowed (e.g., read-only, create, delete or modify).

c) Computing Resources: Includes, but is not limited to, computers, laptops, tablets, workstations, servers, copiers, printers, scanners, faxes and electronic storage media. Computing resources can be dedicated to a single user or can be configured as a shared resource on the network to allow multiple users access to selected drives, files, features or data.

d) Data: Data includes the content of information systems, information in electronic or non-electronic (paper) format, stored/captured audio communications, video tapes, email, instant messages and network resources.

e) Decentralized System: Any data system or equipment containing data deemed private or confidential or which contains mission-critical data, including departmental, divisional and other ancillary system or equipment that is not managed by central ITS.

f) Encryption: A procedure used to convert data from its original form to a format that is unreadable or unusable to anyone without the tools/information needed to reverse the encryption process.

g) File: A collection of data stored in one unit, identified by a filename. It can be a document, picture, audio or video stream, data library, application, or other collection of data.

h) File Sharing: The sharing of computer data or space in a network with various levels of access privilege. File sharing allows a number of people to use the same file by some combination of being able to read or view it, write to or modify it, copy it or print it. Users may all have the same or may have different levels of access privilege.

i) Folder: Folders store files and other folders on a computer. The folders, often referred to as directories, are used to organize files on a computer.

j) Groups: Sets of users.

k) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customer. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

l) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

m) Multi-function Device (MFD): An office machine which incorporates the functionality of multiple devices in one and generally provides centralized document management/distribution/production. A MFD is sometimes called a multifunction printer (MFP), all-in-one (AIO) device and network printer. A MFD may act as a combination of some or all of the following devices: printer, copier, scanner, fax and email.

n) Password: Any secret string of characters which serves as authentication of a person's identity and which may be used to grant or deny access. Passwords are classified as Level 1 Confidential data.

o) Peer-to-peer File Sharing: A term that typically refers to a file sharing network in which shared files are stored on a users' computer where they can be accessed by the other users on the network.

p) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential data and Level 2 Internal Use Data.

q) Shared Network: A network that is shared by multiple users.

r) Shared Resources: A device or piece of information on a computer that can be remotely accessed from another computer, typically via a local area network or an enterprise Intranet, transparently as if it were a resource in the local machine. Examples are shared file access (also known as disk sharing and folder sharing), shared printer access (printer sharing), shared scanner access, etc.

s) SharePoint: A secure customized web portal; allows for assigned community access to documentation, ability of participants to modify documents and online discussion groups.

t) Single User Device: An electronic device, such as a tablet (i.e., iPad), to which multiple user accounts cannot be created and access to information cannot be blocked.

u) User: Users are one or more of the following:
- Anyone or any system that accesses Cal State L.A. information assets.
- Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community.
- Individuals who are given access to sensitive data, have a position of special trust and as such are responsible for protecting the security and integrity of those data.

4 Guidelines

Computing resources can be shared in multiple ways. One way is to share the physical device by allowing multiple users to access it (e.g., a copier or multi-function device (MFD) with multiple users). Another way is to allow designated users access to the files on a shared computer resource (e.g., a user's desktop, decentralized system or department server).

The following general guidelines relate specifically to shared resources:

- Fully understand the sensitivity of the data, function or operation being stored or accessed on the shared resource and implement appropriate security measures.
- Remove or disable unneeded services and software on shared devices, especially those that are network accessible.
- Provide access to only those persons who are otherwise authorized to use the shared resources.
- If appropriate, assign permissions to groups (e.g., department, project group, etc.) not to individual user accounts. Assigning permissions to groups simplifies the management of shared resources because users can be added to or removed from the groups without having to reassign permissions.
- Require all users on shared resources to be individually identified and authenticated before access is allowed so that any actions are separately auditable.
- Remove data from a shared resource once that data is no longer required by deleting the file and emptying the recycle bin, if applicable. Note: if you are sharing a resource in a document library (e.g., SharePoint) and "versioning" is turned on, there could be multiple copies or "versions" of the document that need to be removed
- Securely remove data from the shared resource once that device is no longer required in order to prevent unauthorized disclosure of the shared data. See *ITS-1021-G User Guidelines for Data Sanitization* for information on securely removing data from computers and memory devices.
- Do not leave the password for the "system administrator" account blank or create a simple password (e.g., 1234, sysadmin, etc.). This leaves the computer vulnerable to security breaches because any user can log on to a shared device as the system administrator using a blank or too obvious password. The system administrator password must be changed upon separation of any authorized system administrator. See *ITS-2008-S Password Standards* for information on creating secure passwords.
- The standard security principle of least privileged access must be used on shared resources. For a particular process, application or program, a shared user must only be able to access the minimum information and resources that are immediately necessary to perform job responsibilities, and all controls must be reviewed periodically to ensure continued accuracy.
- Configure a MFD with hard disk storage and that scans Level 1 Confidential Data with clearing capabilities to clear the hard disk between jobs. Clearing the disk between jobs for a MFD that scans Level 2 Internal Use Data is recommended but optional.
- Provide a lock mechanism and prevent physical access to the hard drive of a MFD with a hard disk drive that scans Level 1 Confidential Data. The use of a locking mechanism on a MFD that scans Level 2 Internal Use Data is recommended but optional.

4.1 Use of a Single User Device by Multiple Users

A computer device does not necessarily have only one user. It is not uncommon for several individuals to use the same device. Shared devices offer a cost-effective means to provide users with access without providing individual equipment. A shared computer device needs appropriate security. In fact, when several individuals use the same device, the security risk for all users increases.

Users who share a device that only allows a *single user logon* (e.g., iPad) should:

- Clear the Internet browser history, cookies and cache.
- Disable the option to autofill browser field.
- Not transmit or store protected data on the device.

Users who share a device *with separate logons* should:

- Log off the account when the resource is no longer being used.

All users who share a device should:

- Log out of programs and Internet locations before leaving a shared computer resource.
- Regularly delete unneeded files.
- Refrain from any use that overloads or otherwise negatively impacts the performance of the University computing resources.

4.2 Access to Shared Resources by Multiple Individuals

A file on a computer can be remotely accessed from another computer transparently as if it were a resource in the local machine. This means that one or more individuals can have access to files not located on their primary computer resource.

4.2.1 File Sharing Technologies

There are multiple technologies to use for sharing University files. Below are the recommended technologies and the specific circumstances for the use of each technology:

If you need to:	And don't need to:	Technology to Use
• Send small files, one-time, to one address or a small number of people.	• Share attachments to a list or large number of people. • Share a file with Level 1 Confidential Data and Level 2 Internal Use Data (protected data).	• An email attachment • Removable media (e.g., USB devices, CDs, DVDs, etc.)
• Share files containing protected data. • Share files that need to be sent to a large number of people.	• Allow public access to files.	• SharePoint • Shared Resource

If you need to:	And don't need to:	Technology to Use
• Share files among co-workers within a department. • Collaborate with other faculty members and staff for committee or team projects.		
• Share departmental information that may require enhanced security administration due to the nature of the information or may represent a possible target for intruders.	• Allow access to any person outside the department.	• Decentralized system • Department or central file server
• Share information of a "public" nature, use or general interest to all or a portion of the campus (e.g. bulletins, announcements, forms, reports of general interest, etc.).	• Share a file with protected information. • Share an individual's email messages. • Include list serves or daily deliveries of newspapers. • Include information older than two years unless it is still pertinent.	• University Calendar • University or department webpages • *myCSULA Portal*
• Deploy course materials.	• Save or share any non-electronic documents.	• Moodle

4.2.2 Sharing Methods

There are two methods of sharing files and folders: centralized and peer-to-peer. A shared network may be configured as either a centralized or peer-to-peer network.

- Centralized sharing uses a central file server where all the shared files and folders are stored. To get to the files and folders users first must have access to the central file server. SharePoint and Moodle are all examples of centralized sharing.
- Peer-to-peer sharing is where shared files and folders are stored on a user's computer and other users on the network can access them.

  NOTE: *Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, games and other published materials, is a violation of federal law. It may carry significant monetary and/or criminal sanctions. It is the responsibility of the user downloading or uploading files to ensure that these are not copyrighted works, or that he or she has the permission of the copyright holder. Detailed information is available in ITS-1016-G User Guidelines for Protecting Electronic Copyrighted Material.*

4.2.3 Sharing Files from a Computer

The most common way to share files and folders is to share them directly from a computer, most commonly a department or central file server (centralized sharing). This way, files can be shared from any folder on a computer. Either method allows access to the files or folders from another computer on the same network. However, sharing by these methods should be used with care as there are security implications, such as users copying a confidential or proprietary file to the shared resource that now becomes accessible to other unauthorized users.

Sharing files from any folder on a user's computer (peer-to-peer sharing) is not advised since it can potentially allow unauthorized individuals to take control of the computer if not configured properly, allowing them to install keystroke loggers and other malware, and gain access to passwords, accounts and files.

It is preferable to create and copy or move files to a SharePoint community and grant access to approved users. Using SharePoint allows:

- The simplicity of sharing files and folders from a single location on a computer.
- The ability to quickly see everything that has been shared with others.
- Everything remains separate from a user's Documents, Music and Pictures folders.
- Documents can be checked out, edited and returned, providing an audit trail of revisions.
- Only one person can edit a document at a time, preventing conflicting document versions.
- Everyone has access to the latest document version.

4.3 Restricting Access

Access to shared resources can be controlled by sharing permissions, managing access control, or a combination of these methods. It is important to realize, however, that misuse of remote access functionality can result in a total compromise of a computer, everything stored on it, everything typed into it, and everything accessed from it.

When there is a need to share a resource with others, the file and directory permissions must be set correctly. It is recommended that file and print sharing be disabled unless there is a specific purpose for its use. If file sharing is enabled on a computer, permissions must be set correctly when creating new folders so folders aren't left open to everyone on the network. Do not set up a printer, folder or file to be shared by "Everyone." Sharing with "Everyone" is known as an "open share," which means anyone can access that item.

Information describing how to establish file sharing and security settings is often available in vendor's equipment installation and set-up documentation, or online at the vendor's website, ITCs, ITS staff and the ITS Help Desk are also available to assist support staff.

Users participating in a campus Information Security Program (i.e., Identity Theft Prevention, Payment Card Industry Data Security Standard (PCI DSS), Gramm Leach Bliley Information Security and Health Insurance Portability and Accountability Act (HIPAA)) should consult with the appropriate program coordinator, officer or administrator before allowing access to any shared resource.

Other users should consult with their department Information Technology Consultant, IT support staff, student assistant or department employee responsible for system installation and set-up before allowing access to any shared resource.

4.4 Encryption of Shared Resources Containing Protected Data

Shared resources that contain Level 1 and Level 2 protected data must be encrypted and have an associated encryption key plan in place. The tools and practices outlined in *ITS-2017-G User Guidelines for Encryption Security* must be followed to protect shared resources that contain protected data.

5 Contacts

a) For questions regarding specific departmental procedures and assistance in sharing resources contact the academic or administrative Information Technology Consultant (ITC).

b) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

6 Applicable Federal and State Laws and Regulations

Federal	Title
NA	
State	**Title**
Executive Order S-16-04	**Peer-to-Peer File-Sharing** http://gov.ca.gov/news.php?id=3366 This Executive Order requires the State Chief Information Officer to develop a statewide policy regarding the use of peer-to-peer file-sharing programs on state computers.

7 Related Documents

Cal State L.A.	Title
ITS-2524	**Cal State L.A. Information Security Program** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/campus_information_security_plan_2012.pdf This document establishes the University's Information Security Program in compliance with the *CSU Information Security Policy* and recognizes its obligation to protect the technology resources and information assets entrusted to it.
ITS-1001-G	**User Guidelines for Network Traffic Management** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1001-g_networktrafficmgmt.pdf This guideline helps users meet established network bandwidth allocations and traffic standards to ensure that all University network and technology resources are managed securely.

ITS-1016-G	**User Guidelines for Protecting Electronic Copyrighted Materials** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1016-g_guidelines-protectcopyrightedmaterials.pdf This guideline outlines the steps the campus takes when receiving copyright infringement notifications, settlement letters or preservation notices from copyright holders or their representative agents.
ITS-1027-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1027-g_encryptionsecurity.pdf This guideline provides information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.
ITS-2006-S	**Information Classification, Handling and Disposal** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-2006-s_information_classification_handling_and_disposal.pdf This standard identifies the three levels of information classification and outlines the best practices for handling and disposing of protected data.
ITS-2011-S	**User Access Control for Decentralized Systems** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-2011-s_user_access_control_for_decentralized_systems.pdf This standard describes the system and user access security requirements for decentralized systems that contain University protected data.
ITS-2013-S	**Standards for Utilization of Multi-function Devices** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-2013-s_utilization_multi-function_devices.pdf This standard describes the information security risks of multi-function devices and provides the security requirements for evaluating, implementing, maintaining and disposing of MFDs.
ITS-2823	**Access and Compliance Form** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/forms/its-2823.pdf This form is available for departments with decentralized systems that may require users accessing the decentralized system to sign a formal access and compliance agreement.

ITS-2824	**Decentralized Systems Quarterly Review** http://www.calstatela.edu/its/services.php (under Information Security and Compliance > Decentralized Systems) This form is required for departments that maintain and manage decentralized system to meet audit compliance requirements for a quarterly review of user access controls.
ITS-8824	**Shared Network Resource Request** http://www.calstatela.edu/its/services.php (under Networking) This form is used to request a shared department directory or other network resources.
Chancellor's Office	**Title**
ICSUAM 8000.0-8095.0	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies and standards governing CSU information assets.
CSU Executive Order 999	**Illegal Electronic File Sharing and Protection of Electronic Copyrighted Material** http://www.calstate.edu/EO/EO-999.html This Executive Order specifies that resources of the California State University, including computer hardware and software and intra/inter-campus network connections, must not be used for the purpose of illegal downloading, copying or use of copyrighted materials, including, but not limited to music, videos, motion pictures and Internet accessible content.
Miscellaneous	**Title**
NIST	**User's Guide to Securing External Devices for Telework and Remote Access – Special Publication 800-114** http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf This document provides National Institute of Standards and Technology (NIST) recommendations for securing external devices for telework and remote access.