

## CLA-OIT Securing Private Data Implementation Plan

*Part of the CLA Securing Private Data Standard*

The CLA Securing Private Data Standard specifies that CLA-OIT will establish a basic implementation plan for adhering to the University Securing Private Data Standard. This document represents the default plan for all CLA computers.

All regional technicians and other technical support personnel in CLA-OIT will follow these rules while supporting computers and related technology. Units that employ their own technical support personnel are required to implement this standard or submit an alternative plan for supporting technology in their unit for review and approval.

### General Principles of this Plan

CLA-OIT Regional Technicians are charged with two tasks 1) ensure that steps are taken to protect user data from catastrophic loss and 2) ensure that all clauses of the University and College standards are implemented on all supported computers in CLA. This document explains how CLA-OIT implements solutions for each of the 18 requirements in the University standard. It is important to note that this plan is not intended to meet more stringent University policies and state/federal laws such as HIPPA.

### General Overview of Remote Management in CLA-OIT

With the combination of special network-based software tools, specific configuration settings, and appropriate access privileges, it is *possible* for technicians to do all of the following without physical access to computers:

- patch/update software
- install new software packages
- collect inventory information
- scan for vulnerabilities to network-based attacks
- control and/or observe activity on computers
- search the contents of a hard disk
- without opening, viewing, or reading the contents of any document, use technology tools to scan for files that may contain highly sensitive and legally protected private data (e.g. social security numbers, credit card numbers)

The following are tasks that CLA-OIT Staff *will do* without further notification to users:

- Check computer settings for compliance to University standards
- Correct computer configurations and install/remove software to resolve security issues before University security monitoring terminates network access

The CLA-OIT regional technicians and other staff members will not do any of the following without specific consent from users and/or their supervisors:

- Open, view, or read documents in user home directories or unit shared folders

- Prevent the operation of “disfavored” applications (i.e. software that is difficult to maintain or of seemingly limited value but that does not violate University or College policy). Note: not preventing the use of such software is not the same as providing support for it.
- Correlate software license purchasing records to recorded installations. This is currently the responsibility of the users and units.
- Remotely observe a user’s screen or control a user’s mouse/keyboard.
- Log into a computer using another user’s username and password (including resetting a user’s password to gain access).

## Implementation Plan

### Requirement #1) Local data owner

#### University standard:

Computers and other devices must have an identified local data owner (such as the principal user of the data or the unit supervisor) who is responsible for the data and can act as a point of contact.

#### CLA-OIT implementation plan:

- a. All computers purchased with university funds (e.g. O&M, Fees, ICR, grants, etc.) and used by CLA faculty, staff, and/or students will be entered into CLA-OIT inventory management system (i.e. CLAIM).
- b. A primary user or department contact must be identified for each computer.
- c. Entry in the inventory management system is a prerequisite for a computer to receive technical support from CLA-OIT.
- d. The network name for all computers will be as follows: “4 char unit abbreviation” – “9-digit property ID/asset tag number” (e.g. ABCD-123456789)
- e. Each inventory record requires the following information:
  - o Serial number
  - o Property ID/asset tag number
  - o MAC addresses for all network connections
  - o User/local data owner
  - o Location
  - o Name of the governing Securing Private Data Implementation Plan
- f. Each time a computer is moved (primary home location for laptops), its corresponding record in the inventory management system must be updated accordingly.

### Requirement #2) Technical support required

#### University standard:

Computers and other devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures by a full-time information technology professional, such as competent local information technology support staff. These reviews must include adherence to baseline security requirements as well as additional strategies for protecting the information.

**CLA-OIT implementation plan:**

- a. CLA-OIT provides technical support for all computers that meet the following requirements:
  - o purchased with university funds,
  - o less than three years old,
  - o having configurations equal to or greater than CLA-OIT minimum specifications at time of purchase,
  - o on campus. (Computers that are used off campus must be brought in to campus to be supported by technicians.)
- b. Departments that opt out of CLA-OIT service or that use computers not supported by CLA-OIT must provide alternative professional technical support. Acceptable alternatives include university-employed IT professionals/specialists or contracted support services with central OIT or another university unit. All CLA-OIT technicians and departmental alternatives must adhere to University and CLA-OIT Securing Private Data Standards as outlined in this document.
- c. Technicians will perform routine security checks via remote tools at least every six months.
- d. CLA-OIT can support computers that no longer meet minimum support requirements with special written permission from the CLA-OIT Director of IT Services. An alternative Securing Private Data Implementation Plan will be required, as well as detailed justifications for why the computer cannot be replaced with hardware that does meet minimum qualifications.

**Requirement #3) Staffing level**

**University standard:**

Units are responsible to have appropriately supervised professional technical support staffing sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of private information for which they are responsible and the level of risk. See the Information Technology Support Staffing Standard and the related Information Technology Support Guideline for additional information.

**CLA-OIT implementation plan:**

- a. The college will provide sufficient IT professionals to support college computers according to the University standards and guidelines.
- b. College units providing alternative support must also meet expectations outlined in the Information Technology Support Guideline.

**Requirement #4) Configuration**

**University standard:**

Computers and other devices must be set up in accordance with applicable University security guidelines and standards. As received from the vendor, computers and other devices are not configured for security and require initial as well as ongoing review of the configuration and security of the operating system and software.

- For Windows desktop systems, the Windows Basic Security Guidelines and the Windows QuickStart Security Settings (both Basic & Level-2) are required initial steps. Equivalent settings are required for servers (with adjustments for log size, etc).
- For Mac OS X desktop systems, the Mac OS X Security Guidelines are required initial steps. Equivalent settings are required for servers.

**CLA-OIT implementation plan:**

- a. All computers will adhere to security settings as specified in the University standard specified above.
- b. The CLA-OIT Service Desk will install a standard image onto all new computers that properly configures each computer according to University standards. The Service Desk can also install custom images that meet University standards.
- c. Computers not initially configured by the Service Desk are to be first wiped clean of all vendor-installed software and either have all required software installed manually or via a standards-compliant image.
- d. Technicians who do not use the Service Desk imaging services are asked to have unit-specific images/procedures reviewed by a supervisor once a year.

**Requirement #5) Maintenance and patching**

**University standard:**

Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance must be performed to protect private data (see the Security Patch Standard). Automatic settings or centralized updating of security patches is recommended for most desktop computers.

**CLA-OIT implementation plan:**

- a. All computers are set to receive and install software updates directly from the vendor or via one of CLA-OIT's patch management servers (e.g. Patchlink or ARD Task Server) at a minimum of once every month.
- b. Reports on the "patch status" of supported computers will be provided to technicians on a regular basis.
- c. Technicians will ensure that all critical patches are applied via remote tools or manually within one month of availability.

**Requirement #6) Authentication**

**University standard:**

Access to private data must be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user (see authentication definition below for further detail). Administrator or root level passwords should be exceptionally strong, since these accounts allow complete control of the system. User accounts with fewer privileges should be used instead of root accounts whenever possible. Periodic review of access (through the authorization processes) for databases and tables that are multi-user and outside of the scope of those "centrally-administered" is required.

*Authentication* - Proving that a device or person is who they say they are. The most common form of authentication is a user-id and password. The computer or electronic device must be capable of providing authentication. Some operating systems such as Windows/98 are incapable of differentiating access privileges by user and therefore should not be used for storing private data.

**CLA-OIT implementation plan:**

- a. All computers will require a username and password to log in—automatic-logins are not allowed.
- b. Shared/guest accounts are only allowed on computers when another method is used to determine who has access at any certain time (e.g. laptops checked out from the Service Desk, lab stations reserved in advance, etc.). No private data will be stored on a computer with shared accounts. Shared accounts will have only a minimum of access privileges.
- c. Users will have basic or “power user” access privileges to computer settings. “Power user” privileges will provide abilities to attached peripherals, connect to networks, and other traveling needs but will not permit alterations to security settings as defined in University Standard Requirement #4.
- d. Users can request “administrator access” for special situations. Request must be submitted in writing and approved by the CLA-OIT’s Director of InfoTech Services.
- e. Passwords for user accounts must meet or exceed minimum requirements as defined in the University’s Password Standard.
- f. Accounts with full administrator access to computer settings require complex passwords (as defined in the Password Standard) of 15 characters or longer.
- g. Usernames and passwords for CLA-OIT support accounts will be unique for each region or department.
- h. Default administrator accounts established by the Service Desk during initial setup will be deactivated when the region/department account is established.
- i. Passwords for user accounts assigned to a specific person cannot be shared with other individuals including co-workers, administrative staff/assistants, or family. Units are asked to plan ahead and find alternative options before email and other files must be retrieved during someone’s absence (examples include department email accounts, shared network folders, etc.).
- j. Every shared database stored on CLA servers must have an “access plan” that defines the types of data stored and the access privileges for individual or groups of users.

**Requirement #7) Encryption**

**University standard:**

If sent across the Internet (external to the University's network) or other open networks such as wireless connections, both the authentication data (e.g. a userid and password) and the data itself must be encrypted with strong encryption. Encryption of private data stored on laptop computers or other portable devices is required. An offsite plain-text backup version in a secure location is recommended to protect against lost encryption keys. The University's wired network is not considered an open network.

**CLA-OIT implementation plan:**

- k. Users are strongly advised to store all private data on CLA-OIT servers and not on local hard drives.
- l. All laptops and high-risk desktop computers will be encrypted with Utimaco's SafeGuard Easy (PCs) or FileVault (Macs).
- m. Private data should not be sent via email unless special encryption software is installed and configured on both the sender and recipient computers. (Currently, the University does not offer this service encrypted email service.)
- n. All university-related email accounts will be configured to use SSL.
- o. All computers with wireless network cards will have a copy of the VPN client software installed, configured, and easily accessible.
- p. All encrypted computers will be backed up according to Requirement #14.
- q. No private data will be stored on handheld devices. Email with private data received on handhelds will be deleted immediately after being read.
- r. No private data will be stored on USB flash memory drives or other removable media.
- s. Off campus network connections and on campus wireless connections to CLA-OIT servers must be through a secure VPN connection.

**Requirement #8) Anti-virus technology**

**University standard:**

Desktop and laptop computers must have anti-virus software or filters installed and updated daily (automatic updates recommended). In addition, other Windows computers, including servers, must have anti-virus software installed and updated daily. (See the Anti-Virus Standard).

**CLA-OIT implementation plan:**

- a. All computers will have university-licensed Symantec AV software installed and configured for automatic updates.

**Requirement #9) Firewall or filtering**

**University standard:**

A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to limit network access to the device storing private data. (See the OIT Microsoft Filtering QuickStart).

**CLA-OIT implementation plan:**

- a. Firewalls built-in to the operating system will be active on all computers.
- b. Default firewall configurations will only allow ports and services necessary for common University activities, e.g. email, web, fileserver access, and printing.

**Requirement #10) Access**

**University standard:**

Physical access to computers must be restricted as much as possible. Devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops must be physically restrained (e.g. via an anchoring device) at workstations and servers must be in an appropriate and secure physical facility (see Server Installation Guidelines). Password protected screen saver programs should be used in open locations. Password protected screen savers are required in units identified by the University as "Health Care Components" under the HIPAA regulations and should be set at 15 minutes or less.

**CLA-OIT implementation plan:**

- a.
- b. Users without administrator-level privileges working on desktop computers in a private office will be prompted to re-authenticate after 30 minutes of inactivity.
- c. Users with administrator-level privileges, users working on laptop computers, and users in shared offices will be prompted to re-authenticate after 15 minutes of inactivity.
- d. Unattended desktop computers will be secured behind locked doors and/or with cable locks.
- e. In addition to locked doors, unattended laptop computers will be secured in locked drawers/cabinets or with cable locks.
- f. All college servers will be housed in the University Data Center in WBOB or the secure CLA-OIT server room in Anderson Hall.

**Requirement #11) Security event logging**

**University standard:**

Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs). See Information System Activity Review procedure below. The Windows XP/2000 security setting in the QuickStart "Level-2" Security Wizard sets up security logging.

**CLA-OIT implementation plan:**

- a. All computers will be configured to retain security log files for 90 days.
- b. Log files will be reviewed when there is suspicion of unauthorized access or activity.
- c. Servers will adhere to a separate securing private data plan with more stringent event logging requirements.

**Requirement #12) Reporting Critical Servers**

**University standard:**

Servers storing private data must register with OIT Security & Assurance as "critical servers" and be scanned regularly with vulnerability testing software with corrective actions taken as appropriate. Registration of the server can be accomplished by completing the online form, see Critical Server Identification for more information.

**CLA-OIT implementation plan:**

- a. No computer will be operated as a server unless under direct control of CLA-OIT system engineers or University support services.
- b. All CLA-OIT servers will be treated as a “critical server” and configured and reported accordingly.

**Requirement #13) Vulnerability scans**

**University standard:**

Desktop vulnerability scans are regularly sent to professional technical support staff upon their request for review. Servers storing private data are scanned regularly with vulnerability testing software with corrective actions taken as appropriate (see Notes section below for information on the scan process).

**CLA-OIT implementation plan:**

- a. CLA-OIT IT Services staff will request that each standard CLA-OIT image be scanned for potential vulnerabilities twice annually by OIT Security.
- b. CLA-OIT IT Services staff will coordinate regular vulnerability scans with OIT Security of random computers in CLA.

**Requirement #14) Backups**

**University standard:**

Periodic backup copies of software and data must be made, tested, and stored securely. The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems.

**CLA-OIT implementation plan:**

- a. All computers with locally stored data will be configured for weekly (or more frequent) backups.
- b. All files related to University business will be replicated onto CLA-OIT managed servers.
- c. Server-based storage will be backed up by central OIT.
- d. Backup of files not related to university business is not guaranteed or specifically offered.
- e. Significant amounts of personal files (e.g. music, movies, photos, etc.) are not to be backed up to college servers.

**Requirement #15) Disposal of data and equipment**

**University standard:**

A “secure deletion” program must be used to erase data from hard disks and media prior to transfer or disposal of hardware. (See secure deletion). Permanent media (e.g., CDs, etc) must be physically destroyed.

**CLA-OIT implementation plan:**

- a. At the expiration of support (generally three years after purchase if not otherwise specified), all computers owned by the college must be returned to the Service Desk for proper disposal.
- b. The hard drives of all computers slated for disposal will be wiped with a secure deletion program.
- c. Any computer returning to service in the college will be recorded as such in the inventory management system. This includes supplemental computers used by technicians for testing/support purposes.
- d. Computers will be donated to local schools, handed over to University Computer Services, sold to resellers, or, in limited circumstances, retained for parts.
- e. Retired computers will not be kept in technician offices until processed by the Service Desk.
- f. Computers transferred from one user to another will also be wiped and re-imaged before continued use.
- g. At the expiration of CLA-OIT support, a unit may elect to continue use of a computer only by providing and documenting alternative support according to Requirement #2.
- h. Should a user wish to purchase a computer slated for disposal, the computer must first be wiped clean and re-imaged with a minimal image (i.e. without software packages licensed for University use only). The computer will be sold to the user for fair market value plus tax.
- i. If a computer is to be used exclusively or primarily off campus for university-related business, an alternative support arrangement must be documented and approved according to Requirement #2.

**Requirement #16) Limit services**

**University standard:**

Services available on computers or other devices must be as limited as possible. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to private data. Unless a high level of expertise is available and these services are closely monitored at all times, this higher risk software should not be installed.

**CLA-OIT implementation plan:**

- a. CLA-OIT standard images are configured with essential software packages only.
- b. No sharing services are activated on user computers. If possible, such software will not be installed on the image.

**Requirement #17) Training**

**University standard:**

Training provided by the University on data security practices must be completed by both new and existing employees. In certain units (e.g. units subject to the HIPAA and other regulations) University community members in addition to employees are also required to complete training.

**CLA-OIT implementation plan:**

- a. CLA faculty, staff, and students will participate in University securing private data training programs.
- b. CLA-OIT staff will participate in additional security training (e.g. University HIPAA online courses).

**Requirement #18) Additional actions**

**University standard:**

One or more of the following additional actions should be used to further protect private data, depending upon the situation and requirements:

- a. Limit storage of private data to a hardened file server at the department or collegiate level
- b. Severely restrict the volume and duration of the information stored
- c. Move the data to a dedicated computer with no other applications or data
- d. Limit network access to a list of specific machines or devices (access control list)
- e. Use an internal University, non-routed IP address or network which prevents any access either to or from the Internet
- f. Encrypt stored data (with a clear-text version on a removable medium stored in a safe place)
- g. Sign up for notification of security patch availability from vendors
- h. Separate any sensitive data from other data and store independently (e.g. on a non-networked device)
- i. Develop a security plan

**CLA-OIT implementation plan:**

- a. CLA-OIT file servers are only accessible from within the University network or via VPN. (response to 18e)
- b. CLA-OIT is encrypting laptop storage now and plans to encrypt all locally stored data in the future. (response to 18f)
- c. Service Desk personnel and the Desktop Management Specialist will sign up for security patch notifications. (response to 18g)
- d. This document will serve as the CLA-OIT security plan. (response to 18i)