CALIFORNIA STATE UNIVERSITY
FULLERTON

Computer Classroom Security Standard

Cal State Fullerton operates a heterogeneous network environment composed of centrally supported workstations, servers, and the network infrastructure. Along with administrative systems, the University also operates computer lab facilities which fall into 6 traditional types.

1. Computer classrooms that contain multiple student workstations and are used for computer-related training and other types of class activities
2. Computer classrooms that are owned by departments and used for training.
3. Smart Classrooms that have only one computer installed for presentations.
4. Open, walk-in Public computer labs.
5. Specialty Labs
6. Restricted lab facilities.

Of these 6 types, most labs use Intel based hardware running Microsoft operating systems, Intel or Motorola based hardware running Apple's operating system or hardware running proprietary or non-proprietary variations of UNIX.

The purpose of this standard is to define baseline requirements for the operation of mainstream University computer lab environments to meet CSU security mandates.

Scope:

This standard **fully** covers campus and auxiliary computer classrooms that fall into the following categories:

1. Computer classrooms that contain multiple student workstations and are used for computer-related training and other types of class activities. These rooms are used by various groups and departments and may be used by others who are not CSU Fullerton affiliated (i.e., do not have a Campus Account ID).

2. Computer classrooms that are owned by departments and used for training students of that department.

3. Smart Classrooms that have only one computer installed in the podium at the front of the room.

4. Computer labs that are open to the public (i.e., non-CSU Fullerton users) and not used for training

The above lab types may be exempted from certain requirements of this standard by the technical staff member responsible for the facility by completing and signing the attached addendum and signed certification by an appropriate faculty or management sponsor.

This standard **does not fully** apply to computer labs that are restricted to use by campus personnel/researchers, not used for classroom activities or are configured with specialized hardware and software that cannot be easily enabled to meet existing requirements. Such labs are categorized as Specialty and Restricted Labs.

> Since Specialty and Restricted Labs essentially operate independently from other labs on campus under this standard, there are special considerations that need to be given when classifying a lab as 'Restricted' or 'Specialized'.

1. It is assumed that these labs have operational guidelines and procedures for security and software licensing. As such, these labs will be subject to annual internal audits regarding their security policies for compliance with university, CSU System, and state security policies, as well as software licensing audits to ensure that the labs are in compliance with vendor software licensing agreements.

2. While it is highly recommended that research labs follow as many of the standard's requirements, defined below, these types of labs are not required to meet all requirements of this standard.

Research or specialty labs may be exempted from requirements of this standard by the technical staff member responsible for the facility by completing and signing the attached addendum and signed certification by an appropriate faculty or management sponsor.

Note: While Unix / Linux labs are not required to integrate into the campus Microsoft domains; it is recommended that these labs explore using LDAP authentication through existing ACAD domain structure.

Standard Requirements:

1. Authentication and Tracking

Cal State Fullerton issues and manages University Active Directory Log-In Credentials for all administrative and academic uses.

These Log-In Credentials provide the campus community access to local Rollout Workstations, department provided equipment, computer laboratories, and other campus electronic resources, such as email, Internet access, network printers, network fileservers and data stores. To protect these resources from unauthorized access and use, Cal State Fullerton requires campus users to follow specific guidelines regarding the use and handling of these credentials; see Cal State Fullerton Account and Password Guidelines for modifying user Log-In Credentials.

Lab computers connected to the Fullerton Network must have an authentication mechanism that adheres to the Cal State Fullerton Account and Password Guidelines and uniquely identifies the user of the computer for each session. Before using the lab computer, each user will be required to authenticate via the campus Active Directory domain structure or a local user account with a unique user ID and password credentials which comply with the campus standard. Some method of session time out must be enabled for the user accounts, and a method of logging must be implemented.

Exemption to Authentication and Tracking Requirement

1. Research Lab Facilities

   Research lab systems that are not members of the Administrative; (AD Domain) or Academic; (ACAD Domain), and whose credentials are locally generated must adhere to the Cal State Fullerton Account and Password Guidelines.

   Locally generated accounts must be created and managed by the lab technical staff.

2. Specialized Lab Facilities

   Specialized lab systems that are not members of the Administrative; (AD Domain) or Academic; (ACAD Domain), and whose credentials are locally generated must adhere to the Cal State Fullerton Account and Password Guidelines.

   Locally generated accounts must be created and managed by the lab technical staff.

2. Prevention of the Installation of Malware (Malicious Code)

Each facility must implement steps to prevent malicious code from being installed and executed on the computers**.** In lieu of this, each facility needs to have a documented procedure for installing security updates, monitoring for security threats, and remediation of problems that occur on the lab computers.

Available options:

1) Campus licensed virus prevention and software updating. Contact Campus HelpDesk
2) Disallowing the installation of software by policy restrictions can be used to prevent malware from being installed. Classroom computers can be members of an Active Directory OU(s) to limit activity via Active Directory group policy (GPO).
3) Resetting software such as Deep Freeze by Faronics can be used to control and limit the exposure to malware, and whitelist technology such as Anti-Executable by Faronics can be used to prevent the installation of unauthorized software. Deep Freeze returns the computer to its original state, and Anti-Executable prevents the execution of unauthorized programs.
4) Microsoft Shared Access, Windows SteadyState is another alternative. Available as a free add-in from Microsoft, this utility allows an administrator to control the PC's valid image by defining a restore point in the local group policy.
5) Endpoint security clients can be installed in these facilities.
6) Other technologies that becomes available such as desktop virtualization security solutions (e.g., the use of VMWare) as long as the technology achieves the stated goal of preventing malicious code from being installed and executed on the lab computers.

Example exemption to Prevention of the Installation of Malware Requirement

1. Specialized Lab Facilities running Unix
2. Research Lab Facilities running Unix
3. Operating system not compatible with current virus or patching software.
4. Hardware not capable of running current virus or patching software.
5. Facility is isolated from campus network.

3. Restriction of Privilege

The principal of least privilege must be followed on public computers, and local accounts should not have administrative privilege.

Local accounts and domain user accounts should not have excessive privilege since that puts the machine and user of the machine at risk for infection. If certain software is being used in this facility that requires administrative privilege, then software that allows administrators to run internet-facing applications (such as email clients and web browsers) as a non-administrator should be used.

Exemption to Restriction of Privilege Requirement

1. Lab types 1-4 running applications which can only be run when user is in the local administrator group.
2. Lab types 5-6 running applications which can only be run as a super user or member of the Wheel group

4. Current Security Software

The latest desktop security software available (e.g., anti-virus software from Information Technology or Open Source sites) must be installed and the definitions files must be up-to-date on all computers.

Additional security software such as anti-spyware software should also be installed based on operating system requirements.

5. Physical Security

All computers should be physically secured or access to the facility should be secured through whatever means are fiscally available. Facility entrances should be physically secured when not in use.

All computer facilities should be periodically checked for unauthorized hardware devices (such as hardware key loggers). The frequency and completeness of these checks should be more for facilities that do not have physically controlled access or monitoring. A schedule should be developed which best coincides with the lab environment but periodic checks should be, at a minimum, conducted at least once per month.

6. Signage

There should be visible signage warning the users that they should practice safe computing and not enter their personal information on public or semi-public computers. There should be a standard system banner which appears once users sign on similar to the following:

> *This computer and all University systems accessed from it are for official University use as authorized by* ***UPS 103.004 COMPUTING FACILITIES USE POLICY***
>
> (http://www.fullerton.edu/senate/PDF/100/UPS103-004.pdf).
>
> *All other use is prohibited. All information on this computer system may be monitored by authorized personnel for official purposes. Access or use of this computer system by any person constitutes consent to this policy.*

Enforcement

Computer classroom facilities at the University will be periodically checked to ensure that they are abiding by the requirements set forth in this standard. In cases where the computers are not being properly secured and end users and University network resources are threatened, the Information Security Office, in consultation with the Information Security Officer, will work with the relevant **faculty or management sponsor** to quickly close security holes. In circumstances where these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the public computer facility may be closed and the computers may be disconnected from the Fullerton network by Information Technology Network and Security staff.

Exceptions

Requests for exceptions to any of these requirements may be made by the technical staff member responsible for the facility by completing and signing the attached addendum and signed certification by an appropriate faculty or management sponsor.