IT Security Standard: Computing Devices

Revision History:

Date	By	Action	Pages
09/30/10	ITS	Release of New Document	Initial Draft

Review Frequency:

Annually

Responsible Office:

ITS

Responsible Officer:

Timothy Kearns

CIO, Vice Provost Information Technology

Brief Description:

This standard applies to any university or auxiliary owned computing device.

This standard describes the planning, installation, maintenance, change control, incident response and recovery elements required for computing devices.

Related Policy:

CSU Information Security Policy

- 8045.0 – Information Technology Security
- 8050.0 – Configuration Management
- 8060.0 – Access Controls
- 8080.0 – Physical Security

Cal Poly Information Security Program

Introduction:

Computing devices provide the means to access, process and store information. Compromised access to any computing device threatens the university's information security, including individuals and entities outside of the university. This standard describes the minimum requirements the campus has identified in order to secure the devices at acceptable risk levels.

Scope:

This standard applies to computing devices:

- intended for connection to the Cal Poly data network, or
- containing information as described by the Cal Poly Information Classification and Handling Standard, or
- residing on Cal Poly property or

- managed by personnel in their capacity as a Cal Poly employee or Cal Poly auxiliary organization employee.

This standard exists to ensure that appropriate access, configuration, security and information technology controls are implemented and reviewed on a regular basis.

Standard:

Intended Use Type

In general, computing devices are intended for:

- a single user (e.g. computer, laptop, smartphone)
- multiple users (e.g. computer labs, shared office computers, copiers, printers)
- enterprise services, (e.g. web <servers> and application servers).

Associated Risk

The risk of a breach of data confidentiality, integrity or availability associated with a device depends on the purpose of the device and the information it processes or contains. Risk levels are defined as High, Medium and Low as described by the Information Security Asset Risk Level Definition.

The requirements of this standard are applied based on the intended use and associated risk.

Requirements must be applied to all devices unless noted for a specific use type or risk level.

Required:

Quick Links to sections below (will be hyperlinks to sections when posted on the web):

BEGIN “REQUIRED:” SECTION

1) Documentation

The following information, decisions and processes must be documented by the designated computing device administrator and available for review by the designated management authority.

All Devices

a. Information about the device or storage media
b. Use type and Risk Level

All Devices with Operating System Configuration Access

c. Network services required
d. Network configuration requirements
e. Method used to authenticate users
f. Method used to secure data when traversing the network based on applications and information residing on the device
g. Operating System / Application patch method and schedule. The method must include verification of successful patch installation and remediation process if patch installation is unsuccessful.
h. Operating System and application log scope, review and retention schedules
i. Device and data recovery expectations and procedures
j. Backup schedule and scope
k. Backup retention schedule
l. Recovery test schedule
m. Method and schedule for detecting malicious software
n. Method and schedule for vulnerability testing
o. Computing device decommission date and data disposition date for associated storage media.

Multi-user and Enterprise Computing Devices

p. Process for monitoring activity and responding to information security events
q. Process to make changes (e.g. separation of duties, change approvals, communications plans, change logs, etc.)
r. Process to confirm security configurations prior to deployment and on a documented schedule after deployment
s. Changes to the system (e.g. server administrator’s change log)
t. Process used to grant/change/remove user access. This process must follow the campus Computer Account Standard.
u. Process used to grant/change/remove administrator access. This process must follow the campus Computer Account Standard.
v. Process used to define and approve users/groups/roles and related access to files/programs that ensure the principle of “least user privileges”
w. Incident response expectations

2) Configuration, Maintenance, Access and Change Control

a. Physical placement

All Devices

i. All computing devices and storage media must be located in a space such that when unattended, one of the following controls are in place

1. the device and/or media is protected by entry controls to ensure that only authorized personnel are allowed access to the space containing the device and/or media,
2. the device and/or media is secured in a controlled container,
3. the device and/or media is physically secured to permanent furniture or structures within the space.

Single-user devices storing Level 1 data

ii. Single-user devices storing Level 1 data must be attended or secured with controls to ensure that only authorized personnel are allowed access to the device.

iii. Single-user devices storing Level 1 data located outside of spaces restricted to authorized personnel (e.g. traveling with a laptop) must encrypt the data following the encryption device requirements in section 2f of this standard.

High Risk Enterprise Computing Devices

iv. High Risk enterprise computing devices must be housed in a space with following characteristics:

1. Protected by entry controls to ensure that only authorized personnel are allowed access
2. Access to the space is logged independently from the person accessing the facility (e.g. automated logging technology, receptionist, etc.) and access logs are retained for 30 days.
3. Protected with an appropriate fire notification system and firefighting equipment
4. Cooling that ensures temperatures remain within equipment specifications
5. Uninterruptible power to ensure availability expectations for the device.
6. Communications cabling meets CSU TIP and ITRP Standards

b. System configuration and maintenance

All Devices

i. The computing device must be registered with ITS/Network Administration before attaching to the campus network in a trusted asset or critical asset zone.

ii. A copy of the administrative password(s) must be retained in a secure location by the designated management authority for the computing device.

iii. Computing devices must run operating system versions that are fully supported with pertinent security patches available from the vendor.

iv. Appropriate encryption requirements must be applied for all storage media, (including but not limited to internal, external and portable storage), backup media and data transported across the network.

All Devices with Operating System Configuration Access

v. Computing devices must have controls in place to limit network connections to only authorized users or services (e.g. host-based firewall).

vi. Computing devices must have controls in place to detect and remove malicious software. The controls must be capable of detecting the presence of malicious software at the time of access and during regular system scans. (e.g. anti-malware software capable of live and scheduled scans) . Scans for malicious software must be performed and reported as defined by the method and schedule for the device.

vii. Vulnerability testing must be performed as defined for the device.

viii. The baseline system image must be restricted to read only access except for personnel authorized to manage the image.

ix. Network access during initial installation or upgrades is limited to that which is required to perform the install/upgrade.

x. Network access is restricted to protocols and/or services required to support the purpose of the computing device.

High Risk Enterprise Computing Devices

xi. Network access restrictions using host-based configurations only are not sufficient. These devices must be placed in a Critical Asset Zone to ensure additional network based controls are in place.

xii. A copy of system backups are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the computing device location.

c. Decommissioning and data disposition

All Devices

i. A computing device connected to the campus network must be in compliance with campus standards, even if it is no longer being used for its intended purpose.

ii. Computing devices must be removed from the campus network in a timely way when no longer in use.

iii. Appropriate system and network administrators must be notified of the computing device removal to ensure appropriate configurations changes to those systems and networks.

iv. Disposition of a computing device and/or data must adhere to Disposition of Protected Data and university property control procedures.

v. Data on storage media must be

1. rendered unreadable before requested for survey.
2. rendered unreadable before transfer to another organization, either internal or external to the university, for reuse or repair.
3. kept in a location limited to authorized personnel while awaiting processing to render the storage media unreadable.

d. Patching

All Devices

i. Devices that do not have operating system and/or application patches applied as described in this section may be removed from the campus network.

ii. Operating system and application patching is performed based on the documented method and schedule for the device.

iii. Application of applicable patches is required at least every 90 days unless an exception has been approved by the management authority that includes an appropriate risk analysis and compensating controls.

iv. Security vulnerabilities that can be eliminated by patching the operating system or application must be assessed for risk in a timely way and applied outside of normal maintenance patches unless other compensating controls are in place and approved by the management authority for the device.

High Risk Enterprise Computing Devices

v. Patches must be applied and tested on a test device prior to installation on the device supporting production services.

e. Logging

All Devices with Operating System Configuration Access

i. Audit logs recording user activities and information security events must be kept and reviewed as defined for this device.

1. Log information must include, but is not limited to:
    a. Date/time/details of key events (e.g. log-on/log-off)
    b. Use of privileged accounts (e.g. supervisor, root, administrator)
    c. Successful and rejected system or user access attempts
    d. System and/or application start-up and stop
    e. System alerts
    f. Changes to or attempts to change system security settings.

ii. Log information must be protected against tampering and unauthorized access.

High Risk Enterprise Computing Devices:

iii. Logs must be reviewed based on the process for monitoring activity and responding to information security events.

iv. Logs must be retained on a computer separate from the computing device generating the log.

f. Encryption

All Devices

i. Level 1 data must be encrypted when stored on devices or media that can not adhere to the physical placement requirements or connected to the network outside of a Critical Assets Zone.

ii. Level 1 data must be encrypted when transported across the network outside of a Critical Asset Zone.

iii. Encryption modules must adhere to Federal Information Processing Standards 140-2 or approved by the Information Security Officer.

iv. Encryption key sizes must be sufficiently large to ensure protection from brute force attacks when used with the chosen encryption method.

v. Encryption keys must be protected with passwords that follow the university password standard

vi. Encryption keys must be changed following the same principles identified in the university password and user access standards.

g. Configuration audits

All Devices with Operating System Configuration Access

i. Documented configuration settings are confirmed prior to deployment of the device and at least annually thereafter reconciling with logged changes to the device.
ii. The backup processes are confirmed based on the defined scope and schedule.
iii. Recovery tests are implemented as defined for the device.
iv. A vulnerability scan is completed and issues identified are remediated prior to deployment of the device and at campus standard intervals.
v. User access is confirmed following campus standards.

h. Access

All Devices

i. Unnecessary (default) system accounts are removed and system and administrator accounts changed from default settings
ii. All account passwords adhere to campus password standards.
iii. User access is defined using the principle of "least privilege".
iv. Access to services and/or data is granted via groups/roles.
v. In the event of compromise, all affected accounts (administrator and user) must be revoked and/or passwords changed.
vi. When using elevated privileges:
    1. Elevate only when needed to accomplish a task
    2. Reduce privileges to "least privilege" once the task is accomplished

Multi-user and Enterprise Computing Devices

vii. The number of consecutive invalid login attempts is limited based on the campus password standard.
viii. Sessions are locked or disconnected after a defined period of inactivity, e.g., 15 minutes.

i. Change Control

All Devices

i. Granting, changing and removing access must follow the defined process for the computing device.
ii. Configuration changes must follow the defined process for the computing device.

High Risk Enterprise Computing devices:

iii. Configuration changes must be made on a test computing device and a documented test plan implemented prior to deployment on a production computing device.

3) Incident Response

a. Logs must be reviewed based on the risk assessment for the computing device and system administrators must respond to discovered events following the university incident response standard procedure.
b. System administrators follow campus incident response procedures
c. System administrator(s) log response activities
d. A device may be removed from the campus network by the Office of the CIO if deemed necessary until the risk posed by the device has been removed.

Recommended:

1) Configuration, Maintenance, Access and Change Control
    a. Physical placement

        All Devices

        i. Only store Level 1 data on High Risk Enterprise Computing Devices. The potential for Level 1 data to be compromised can be substantially reduced by only storing Level 1 data on High Risk Enterprise Computing Devices.

        Enterprise Computing Devices

        ii. Protected by entry controls to ensure that only authorized personnel are allowed access
        iii. Protected with appropriate firefighting equipment (e.g. fire extinguisher)
        iv. Cooling that ensures temperatures remain within equipment specifications
        v. Uninterruptible power sufficient to allow operation in the event of a small power outage to prevent hardware damage or data corruption.

    b. System configuration and maintenance

        All Devices

        i. Use of a centralized authentication services
        ii. A copy of system backups are stored in a remote location, at a sufficient distance to escape any damage from a disaster or equipment failure.
        iii. Implement an automated notification system to send system administrator(s) information about key activities such as suspicious events, events that may cause service interruptions (e.g. full disk partitions), failed backups, etc.

    c. Patching

        All Devices

        i. Use of a centralized patching process.
        ii. Patching activities are automated unless specific coordination is required.
        iii. Configuration and patch reporting should include the following:
            1. Compliance (e.g. success/failure of operating system and primary application patches)
            2. Standards (e.g. variance from supported operating system and application versions)
            3. Differences (e.g. changes/trends in the managed computer from the previous report or baseline security standard)

    d. Logging
        i. Retain system logs for at least 30 days but not longer than 90 days unless a longer retention period is needed for specific business processes.
        ii. Retain logs on a computer separate from the computing device generating the log.

    e. Access
        i. Use of a centralized account provisioning services

Definitions:

Administrator Account:

An account on a computing device that allows for all or a broad range of privileges for purposes of administering the device or an application.

Administrative Password(s):

The password associated with the Administrator Account(s).

Devices with Operating System Configuration Access

Devices where the manufacturer allows and expects the owner to manage operating system configuration settings. Devices with operating systems hidden by the manufacturer, such as some instrumentation devices or commodity mobile phones would not fall under this definition.

Enterprise Computing Device or Server:

Any computing device that offers services to more than one user over the network or is used to provide data or services to another device.

Least Privilege:

Offering only the required functionality to each authorized user.

Storage Media:

An electronic device that can hold data. Examples include: disk drives internal and external to a computing device, memory cards, magnetic tapes, and DVD/CD disks.

System Administrator or Computing Device Administrator:

The individual or individuals responsible for the overall implementation and maintenance of a computing device.

Responsibilities:

Designated Management Authority

- Strictly observes all laws, regulations, policies, standards and procedures related to security of information and information technology resources in their area.
- Responsible for and shall take reasonable measures for implementation of, and compliance with, the Information Security Device Standard for devices within their areas.

Computing Device Administrators/Application Administrators

- Strictly observes all laws, regulations, policies, standards and procedures related to security of information and information technology resources in their area.
- Prepares and maintains procedures and documentation in compliance with the Information Security Device Standard for assigned devices.
- Executes device administration procedures in compliance with the Information Security Device Standard for assigned devices.

Computing Device Users

- Strictly observes all laws, regulation, policies, standards and procedures related to security of information and systems used.

- Protects the privacy rights of University faculty, staff and students.
- Protects the physical security of data and systems assigned to them.
- Reports suspected violations of security policies and procedures for the University information to their supervisor who will report it to the Information Security Officer and/or Information Technology Services depending on the nature of the violation.

Non-Compliance and Exceptions:

Systems found in non-compliance with this standard may be removed from the network until they do comply.

If it is technically infeasible for an information resource to meet this standard, departments must submit a request for exception to the VP/CIO and ISO for review and approval.

Related Procedures and Resources:

Information Security Asset Risk Level Definition
Computer Account Standard
CSU TIP and ITRP Standards
IP Address Request form
Network Security Standard
Procedure for Removing a Device from the Network
Disposition of Protected Data
University Property Control Procedures
Cal Poly Password Standard
Incident Response Practice