PURPOSE

Establish procedures and policies for configuration management of information processing platforms and software.

PROCESS

Configuration Management (CM-01)

The College establishes the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during and after system implementation.

Information technology resource owners must ensure vendor-supplied security patches are routinely acquired, tested and installed. Critical security patches must be installed within 30 days of release. Patches categorized as high must be installed within 45 days of release. All other security patches must be installed within 60 days of release.

Information technology resource owners must enable recommended security features included in vendor-supplied systems and must disable or change the password of default accounts before placing the system into use or placing it on the network.

Baseline Configuration (CM-02)

The College establishes baseline configuration of information resources to ensure changes to information resources are executed consistently in the production environment.

The information resource owner must develop baseline configurations of information resources. Configurations settings must be documented so they can be repeatable. Desktop and server operating systems must use golden images of reviewed and accepted configurations. The desktop and server operating systems must also have configured and operating anti-virus/malware software and additional system analytic software based on risk factors as approved by the Chief Information Security Officer (CISO) and information resource owner.

Change Configuration Control (CM-03)

The Change Review Board (CRB) must meet regularly to review upcoming and completed changes. The CRB is minimally composed of the Chief Information Security Officer (CISO), the Division Director of Information Technology, the Director of Applications, Director of Support, and the Director of Infrastructure. Others can serve at the discretion of the Chief Information Security Officer (CISO) and of Division Director of Information Technology.

Change Requests Procedures

A change request is initiated when an operational change is needed to be applied to the current technology. Particular categories, though not all inclusive, include:

Software and hardware patches, installing new versions of software, new software and hardware installation, software configuration changes, changes that involve a system being restarted, changes that must be deployed on multiple client systems, changes impacting client access to a system.

Roles:
Change Initiators- owner of the change. Responsible for filling out the change form, monitoring the assessors and approvers assignments, and updating the status. Initiators should start the process at least a week before the desired time to start implementing the change.

Assessor- for notification and awareness of the change. Evaluates the change and makes comments on how it may impact their systems. Review the description and plan to ensure it addresses concerns on how it will impact their area or systems. Apply a business and technical risk based on their evaluation of the change. Assessors should evaluate the change and ask clarifying questions or provide additional information within 2-3 days after assignment.

Approver- responsible for providing final approval for the change to proceed. The approver is typically a senior administrator or system owner depending on the potential breadth of the change. The approver should allow sufficient time for assessors to complete their assignment before giving final approval.

Items the approver is reviewing-

Roll out and roll back plan is sufficiently detailed, the process is thought out, and the communication plan takes into account impact on other systems and risk mitigation.

The approver should evaluate the assessor’s comments and ensure any concerns that have been brought forward are addressed.

Change form components:
Client ID- system or group where the change will be performed

Change Type-

Normal-password resets

Routine- monthly updates, other changes that have been completed 3 or more times successfully and the description and roll-out plan are the same

Comprehensive- higher impact or new change process

Emergency- a high-impact change in response to an urgent situation

Reason- describe subject or type of change

Proposed Start date- anticipated date change will begin

Proposed End date- anticipated date the change will be completed

Actual end date- date the change is actually completed

Review date- expected change meeting when the results will be reviewed

Change description- describe in detail what needs to be changed. If it is a patch, describe the patch, vendor patch number, and a link to the patch description. For new hardware, describe what is being installed, quantity, part numbers, software name, and version. The description should be detailed and not a summary. If the description is lengthy, then summarize and attach additional details to the change.

Describe what systems and services will be impacted by the change. Will certain applications be unavailable and to what extent? Will certain hardware be added and removed?

Reason for change- describe the reason the change is needed. Patches can be to fix a security or software bug. New hardware or software to bring a new service into production or to replace existing systems.

Risk- Describe the risk to business operations this change will/may have.

Impact Assessment- Describe what systems will be impacted by this change. List applications on the affected system and what inter-connected systems will be impacted. Describe the impact to each system.

Implementation plan- Describe in detail how the change will be implemented. In complicated changes, you can attach a document to the change. Answer the following questions at a minimum:

1. Testing procedures- both pre and post
2. What will be done to mitigate the amount of time for the change and impact to users
3. Detail list of what will be done to implement the change (tasks)
4. Date and time
5. Communication plan; what notifications are needed and to whom

Acceptance Criteria- Describe how the system will be tested post-change to ensure the system is fully operational.

Back out plan-Describe how the change can be rolled back in case of problems. Include any extra steps that will be taken to provide a roll-back point in the OS or another backup procedure. Emphasis is on what actions are being taken to minimize business disruption and protect the data.

Implementer's Notes- Any notes about the implementation of the change. Document all unexpected changes.

Review date and Notes- Date a review of the change is completed. Comments should include the success of the change, any unanticipated events and how they impacted operations and notes on any changes that should be made to future roll-out plans. Review should also include the success rate of the deployment of a patch to clients.

Final Disposition Rating- Select one of three options to rate the success of the change

1. **Successful**- change went as planned and no problems were encountered on the system or for clients.
2. **Successful minor complications**- change went as planned but there were minor problems encountered. Generally, these problems would not be service impacting and went unnoticed by clients. Describe in the Review Comments what the complications were.
3. **Successful Major Complications**- change did not go as planned but was completed. Unexpected service interruptions, outage took longer than expected,

clients unable to use system normally, calls to the help desk regarding related problems. Describe in the Review Comments what the complications and impact to clients were.

4. **Rolled Back**- Change did not go as planned and was rolled back. Describe in the Review Comments the complications encountered and success of the roll back.
5. **Canceled**- Change was canceled and not implemented. List reason for cancellation.
6. **Failed**- Change failed and was not able to be rolled back. List what went wrong with the change.
7. **Declined by Change Review Board (CRB)** - Change Board did not approve the change.

Security Impact Analysis (CM-04)

All security-related information resources changes must be approved by the information technology owner through a change control process (CM-03). The change management process must utilize the College's change system/process.

Change approval must occur prior to implementation. Post-implementation security scan should be run to confirm changes.

Configuration Settings (CM-06)

The College:

- establishes mandatory configuration settings for information technology products employed within the information system;
- configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
- documents the configuration settings; and
- enforces the configuration settings in all components of the information system.

These configuration settings are established by Information Technology department and implemented and enforced using a combination of golden images, registry settings and group policies. Documentation for specific software settings is maintained in operation documentation repository and updated regularly.

Least Functionality (CM-07)

The College configures information technology systems to provide only essential capabilities. The use of configuration settings (CM-06) incorporates the least-needed functionality by disabling or removing unneeded applications and settings from operating systems and application software.

Information System Component Inventory (CM-08)

The College develops, documents, and maintains a current inventory of the components of the information technology systems and relevant ownership information.

The information technology system inventory and ownership are maintained by the Information Technology department and stored in the IT Help Desk system. The lifecycle of components is recorded including acquisition, installation, repairs and disposal.

Software Usage Restrictions (CM-10)

The College:

- uses software and associated documentation in accordance with contract agreements and copyright laws;
- tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

The Information Technology department maintains an inventory of software licenses. Configuration management software is used to survey devices for software inventory. Network management technologies and settings are used to restrict peer-to-peer file sharing.

User-Installed Software (CM-11)

The College establishes and enforces a policy governing the installation of software by users.

Information Technology department is assigned the responsibility to authorize and install software on information technology systems. All software installed on College-owned or operated computer systems must be licensed to the College for installation and use. Licensing agreements should be maintained by Information Technology department. When agreements are not feasible, sufficient documentation should be maintained to validate the software is appropriately licensed.

*If the Chief Information Security Officer (CISO) and the Division Director of Information Technology are the same individual, the coordination as indicated in the policy requires coordination with immediate supervisor.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.