CPTC IT Procedure: Maintenance of IT assets

The TCSG Information Security Standards are the foundation guidelines for information technology procedures, maintenance, and security in all TCSG entities. The guidelines constitute a set of standards for information technology security to maximize the functionality, security, and interoperability of all TCSG's information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This procedure is designed to help ensure information security due diligence in information security and risk management by identifying tools and processes to safeguard CPTC's assets.

This procedure extends the scope of the TCSG guidelines for greater specificity. Any changes or differences in the TCSG document will supersede this CPTC procedure.

The three main objectives of this procedure are to provide the following.

1. Develop, document and disseminate to authorized personnel an information system security maintenance procedure that addresses the items in the list below:
    a. Purpose;
    b. Scope;
    c. Roles;
    d. Responsibilities;
    e. Management commitment;
    f. Coordination among organizational entities; and
    g. Compliance.

    Authorized personnel are all individuals who have been granted access to IT systems at CPTC. Typically, this will be CPTC IT staff, but it may also be other personnel who are tasked with making repairs or installations on the College's systems. For example, this could be members of the College maintenance division or an outside contractor performing maintenance or repairs on our CRAC units, engineers from our ISP upgrading their CPE, or a cabling contractor installing new network drops in data rooms.
2. Develop and maintain procedures that facilitate the implementation of the information system security maintenance requirements and associated system information system security maintenance controls; and
3. Review and update the current information system security maintenance requirements and procedures at least annually or when significant changes occur.

Responsibilities:

All covered personnel involved in the maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any local maintenance requirements.

Role	Definition
TCSG Chief Information Officer	The TCSG Chief Information Officer (CIO at the TCSG senior leadership level) is assigned the responsibility for providing leadership as well as supporting and promoting information system security maintenance throughout TCSG agencies. (Currently Steven Ferguson)
TCSG Information Security Officer	ISOs are responsible for maintaining the appropriate operational security posture for TCSG controlled information system or program. (Currently Michael Clough)

CPTC Information Security Administrator	The person responsible for implementation and enforcement of TCSG and College Information Security Policies, Standards and Best Practices. This person is the single point of contact for the College for issues involving Information Security. Refer to the TCSG ISS for requirements for being a CPTC ISA. (Currently Derrell Harris)
Information System Owner	An Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The identity of this individual varies with the system. When in doubt, this is the divisional head who requested implementation of the system.
External Service Providers	Organizations are becoming increasingly reliant on information system services provided by external providers to conduct important missions and business functions. External information system services are computing and information technology services implemented outside of the traditional security authorization boundaries established by organizations for their information systems. Examples of these are Cisco (Umbrella), Microsoft (Office 365), Ellucian (Banner), and TCSG Managed Services (Banner). Third party service providers with systems interconnected to the College network are responsible for maintaining their systems in accordance with this procedure. For each service provider identified, the information system owner will provide the contract agreements and service level agreements highlighting the inclusion of security and privacy requirements, data handling restrictions and provisions for regular audits or assessments per GLBA and auditor requirements.

Controlled Information System Security Maintenance

1. Schedule, perform, document, and review records of information system security maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and organizational requirements;
2. Approve and monitor all maintenance activities to include routine scheduled information system security maintenance and repairs, whether the equipment is serviced onsite, remotely, or moved to another location;
3. Ensure removal of the information system or any of its components from the facility for repair is first approved by an appropriate official;
4. Sanitize equipment to remove all information from associated media, following proper procedure, when the information system or any of its components require offsite information system security maintenance or repairs;
5. Verify proper functionality of all potentially impacted security controls after information system security maintenance is performed; and
6. Maintain information system security maintenance records for the information system to include the:
    a. Date and time of information system security maintenance;
    b. Name of the individual performing the information system security maintenance;
    c. Name of escort for outside technicians where necessary;
    d. Description of the information system security maintenance performed; and
    e. List of equipment removed or replaced (including identification numbers, if applicable).

7. Employ automated mechanisms to schedule and conduct the information system security maintenance as required, to create up-to-date, accurate, complete, and available records of all information system security maintenance actions. This requirement is only applicable to HIGH impact systems. The categorization of “HIGH,” “MODERATE,” or “LOW” is defined in Federal Information Processing Standards (FIPS) Publication (PUB) 199.

MA–1 – Introduction

All College and agency information assets should meet the required security controls defined in the NIST SP 800-53, Revision 4, Security and Privacy Controls. This document addresses industry best practices that are helpful in implementing the systems maintenance and controls.

The College has adopted the maintenance principles established in NIST SP 800-53 Rev 5 “Maintenance” control guidelines as additional guidelines for this security domain. The "MA" designator identified in each control represents the NIST-specified identifier for the Maintenance control family. This is identified in the Security Control Identifiers and Family Names table. The provisions of this procedure outline the Maintenance requirements that TCSG and each college must develop or adhere to in order to be compliant with this policy.

To maintain the highest level of system availability and protect the College’s IT infrastructure, maintenance operations must be performed at established and authorized times, on an approved, as-needed basis, or, rarely in cases of emergency, as quickly as possible. Maintenance procedures will be developed and maintained to facilitate the implementation of the Information Technology (IT) security maintenance requirements and associated system information and system security maintenance controls.

MA–2 - Controlled Maintenance

The College will abide by the following to ensure the integrity and security of all IT assets and systems.

a. Establish normal change management and maintenance cycles for all IT assets and systems.
b. Perform maintenance of operating systems in accordance with approved TCSG IT security requirements as well as in accordance with manufacturer or vendor specifications. TCSG requirements will supersede manufacturer or vendor specifications.
c. Consider the following issues when supporting operating systems:
    i. New security risks and vulnerabilities are discovered on a regular basis. They frequently require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.
    ii. Periodic maintenance improves the performance of operating systems
    iii. The operating systems on servers frequently require regular maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded.
d. Ensure that all current maintenance and security vulnerability patches are applied to all affected hosts and that only essential application services and ports are enabled and opened per TCSG Information Security Standards (TCSG ISS)
e. Logs of operating system maintenance will be monitored regularly to ensure:
    i. Maintenance tasks continue to function as expected.
    ii. Operating systems continue to operate within accepted thresholds.
    iii. System security is not being compromised by maintenance tasks.

iv. Maintenance tasks do not adversely affect computer capacity or performance.

f. The College IT staff will ensure that software faults or bugs are formally recorded and reported to those responsible for software support and maintenance.
g. Restrict physical access to systems in accordance with the TCSG ISS. This applies to all server rooms, data rooms, or any other system location not named here.
h. All assess to server rooms and data rooms will be logged in a log book or sheet. These log books or log sheets will be reviewed regularly per TCSG ISS. Preferably, server rooms will have a video camera to record personnel ingress and egress information.
i. When possible, the College IT staff will apply a comprehensive set of monitoring and management tools in order to keep all IT assets and systems up-to-date and detect when they are out of compliance.
j. Monitor information systems (e.g. using Simple Network Management Protocol (SNMP)) so that events such as hardware failure and attacks against them can be detected and responded to effectively.
k. Care should be taken to ensure that the management and monitoring software systems are secure – especially open source software.
l. Review maintenance records on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server (e.g. by inspecting logs).
m. Provide or arrange maintenance support for all equipment that is owned, leased or licensed by the College.
n. Arrange support services through appropriate maintenance agreements or with qualified technical support staff.
o. Schedule, perform, document, and review records of information system security maintenance and repairs on information system components in accordance with TCSG guidelines, manufacturer guidelines, vendor specifications, and organizational requirements.
p. Maintain records of all maintenance activities.
q. Approve and monitor all maintenance activities to include routine scheduled information system security maintenance and repairs, whether the equipment is serviced onsite, remotely, or moved to another location.
r. Ensure removal of the information system or any of its components from the facility for repair is first approved by an appropriate official.
s. Verify proper functionality of all potentially impacted security controls after information system security maintenance is performed.
t. Restrict the use of root/administrator privilege to only when required to perform duties per TCSG ISS.
u. Establish normal change controls and maintenance cycles for resources.
v. Maintain information system security maintenance records for the information system to include the following:
    i. Date and time of information system security maintenance
    ii. Name of the individual performing the information system security maintenance – regardless of whom the provider works for
    iii. Name of escort of outside non-CPTC personnel in sensitive areas, if necessary
    iv. Description of the information system security maintenance performed;
    v. List of equipment removed or replaced (including identification numbers, if applicable);
    vi. Employ automated mechanisms to schedule and conduct the information system security maintenance as required; and
    vii. Use maintenance tools that can create up-to-date, accurate, complete, and available records of all information system security maintenance actions. This

requirement is only applicable for information systems with a “HIGH” impact security categorization based on its impact on critical business processes and the sensitivity of the data contained within the system. The categorization of “HIGH,” “MEDIUM or “LOW” is defined in http://it.nc.gov/document/statewide-data-classification-and-handling-policy

Control: The College:

a. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
b. Staff who perform upgrades will perform checks on potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. Where IT is responsible for the technical but not functional aspects of systems, IT will request that the appropriate personnel perform the tests.

Control Enhancements:

1. The organization maintains maintenance records for the information system that include:
   a. Date and time of maintenance;
   b. Name of the individual performing the maintenance;
   c. Name of escort, if necessary;
   d. A description of the maintenance performed; and
   e. A list of equipment removed or replaced (including identification numbers, if applicable).
2. The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs when possible. This produces up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

MA–3 – Maintenance Tools

The College will approve, control, and monitor the use of information system security maintenance tools and maintain these tools on an ongoing basis. Also, the College ISA or his designee will, to the best of his ability, inspect all maintenance tools carried into a facility by information system security personnel for unauthorized modifications or contain malicious code and handle the incident consistent with State, TCSG and College incident response policies and procedures. All electronic equipment transferred to surplus is received by a company that will securely sanitize all equipment received.

MA–3 (2) – Maintenance Tools - Inspect Media (Moderate Control)

The College ISA or his designee will scan all files and media containing diagnostic and test programs for malicious code before they are used in the information system; If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with TCSG incident handling policies and procedures.

MA–4 - Nonlocal Maintenance

The College will ensure that all nonlocal (remote access) maintenance and diagnostic activities of information systems conducted by individuals through either internal or external network observe the following requirements:

a. Nonlocal maintenance and diagnostic activities are approved and monitored.
b. Where possible, staff and agents will employ multi-factor authentication that combines at least two mutually-independent factors such as challenge / response answers,

biometrics, and tokens, for nonlocal maintenance and diagnostic sessions to protect the integrity and confidentiality of communications.
c. Staff and agents will maintain records for nonlocal maintenance and diagnostic activities.
d. Staff and agents will terminate sessions and network connections when nonlocal maintenance is completed.

MA–4 (2) - Nonlocal Maintenance – Document Nonlocal Maintenance (Moderate Control)

Allow the use of nonlocal maintenance and diagnostic tools only as consistent with State and TCSG policies and procedures. These tools will also be documented in the security plan for the information system.

MA–5 - Maintenance Personnel

The College will ensure that all individuals performing hardware or software maintenance on State or agency information systems have the proper access authorizations needed to connect to networks in order to perform maintenance activities. A common example of this is adding, repairing or upgrading network cabling. The College ISA or his designee will, to the best of his ability:

a. Establish a process for authorizing information system security maintenance personnel;
b. Maintain a current list or log of authorized information system security maintenance organizations or personnel;
c. Ensure non-escorted personnel performing information system security maintenance locally or remotely have appropriate access authorizations to the information system allowing access to State data. This includes an escort where indicated. Inappropriate access would result in a compromise of confidentiality, integrity, or availability; and
d. Designate personnel with required access authorizations and technical competence to supervise the information system security maintenance activities of personnel who do not possess the required access authorizations.

MA–6 - Timely Maintenance

The College will perform preventative information system security maintenance support for the purpose of maintaining equipment and facilities in satisfactory operating conditions.

a. Predictive maintenance, or condition-based maintenance shall be performed by conducting periodic or continuous (online) equipment condition monitoring.
b. Where feasible, automated mechanisms should be used to transfer predictive maintenance data to a computerized maintenance management system. Where feasible, backup systems should be available for critical systems.
c. This control is optional for LOW impact information systems.

Support for Operating Systems

The College will ensure that the operating systems used to run the production environment are regularly monitored for security risks and maintained in approved secure configurations to support business operations. Agencies should consider the following issues when supporting operating systems:

a. New security risks and vulnerabilities are frequently discovered that may require the operating system to be patched or the configuration to be updated to mitigate the identified risks and vulnerabilities.
b. Periodic maintenance improves the reliability and performance of operating systems

c. The operating systems on servers frequently require daily maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain time, threshold or limit is exceeded.
d. Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure that the following:
    i. Maintenance tasks continue to function as expected.
    ii. Operating systems continue to operate within accepted thresholds.
    iii. System security is not being compromised by maintenance tasks.
    iv. Maintenance tasks do not adversely affect computer capacity or performance.

Operating System Software Upgrades

Operating systems (OSs) should be kept up to date to ensure stability and security. Upgrades shall be carefully planned, executed and documented as a project. Teams planning and implementing operating system software upgrades to systems shall perform the following steps before commencement of the upgrade project:

a. Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade.
b. IT will notify all departments affected by OS upgrades with all knowledge they have of changes. This will not be a complete list. IT will notify all affected departments in a reasonable time after learning of upgrades to be performed by outside entities. A prime example of this is Banner upgrades performed by TCSG's Managed Services staff.
d. System users will perform testing after upgrades and communicate results to IT as soon as possible.
e. Establish a rollback plan in the event the upgrade has unacceptable ramifications.

Guidelines

Teams responsible for maintaining operating systems should consider the following security issues when upgrading an OS:

a. An OS failure can have a cascading adverse effect on other systems and perhaps even the network.
b. System documentation and business continuity plans should be amended to reflect the OS upgrade.
c. Since OS upgrades typically affect many systems within an organization, such upgrades should be part of the annual maintenance plan/budget. OS upgrade testing and review cycles should also be included in this budget.

Managing System Operations and System Administration

CPTC systems shall be operated and administered using documented procedures that are efficient and effective in protecting the College's system and data.

a. For IT transaction records, which include access and audit logs related to the activities of IT systems, the college will establish and maintain an adequate system of controls.
b. The College will employ and document controls to provide for the management of system operations and system administration. To minimize the risk of corruption to operating systems or integrated applications, the controls shall include, but not necessarily be limited to, the following:
    i. Develop and document daily operational security procedures.
    ii. Assigned staff shall perform the updating of the operating systems and program/application backups.
    iii. Operating system software patches shall be applied only after reasonable testing verifies full functionality.

iv. Client upgrades are to be automated when possible.
v. Server operating systems shall be either upgraded or reinstalled. The decision to upgrade or reinstall will depend on system complexity, required downtime, and system stability of the outcome.
vi. All Banner OS and application updates and patches will be approved by TCSG's Enterprise Services and installed and monitored by TCSG's Managed Services personnel.
vii. Physical or logical access shall be given to outside agents for support purposes only when necessary and with documented management approval. The agent's activities will be continually monitored.
viii. Vendor-supplied software used in operating systems shall be maintained at a level supported by the vendor. Unsupported software should be either brought under support, sufficiently isolated, or phased out. Unsupported software does not receive patches and upgrades is not secure and may pose a threat to other systems.

c. The college will clearly define security responsibilities for system administrators, who shall protect their assigned information technology resources and the information contained on those resources.
d. The College will provide appropriate training for their system administrators.
e. System administrators will do the following:
    i. Ensure that user access rights and privileges are clearly defined, documented and reviewed for appropriateness.
    ii. Consider the risk of exposure when administering system resources. When in doubt, the administrator should ask the ISA/Executive Director of IT (EDIT) for guidance. If the ISA/EDIT is unsure of the best action, he will consult the TCSG IT department before moving forward.
    iii. Take reasonable actions to ensure the authorized and acceptable use of data, networks and communications transiting the system or network.

Scheduling System Operations

College IT staff will ensure that modifications to information system operations are implemented and maintained properly.

a. Documented operational procedures must be created, implemented and maintained during system operations and take into consideration the following:
    i. Computer start up, shutdown, and recovery procedures
    ii. Scheduling requirements (length of maintenance window, other parties needing to be involved, schedules of other parties needing to be involved, etc.)
    iii. Processes for handling errors and unforeseen issues that may arise during job execution
    iv. Contact lists of supervisors of affected departments. Those supervisors will notify their staff of the scheduled maintenance.
    v. System restrictions
    vi. Instructions for handling output, including failed jobs
    vii. Proper media handling and storage
    viii. Incident handling and escalation procedures
    ix. Configuration management
    x. Patch management. Where and when possible, automated patch management systems are preferable to manual updates.
    xi. General system hardware and software maintenance
b. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.

c. TCSG will notify the EDIT or Banner Main Contact of maintenance performed or coordinated by TCSG. The EDIT or designee will notify supervisors regarding upcoming maintenance. When options are available, the EDIT or designee will request input from other departments before replying to TCSG. When other departments are notified of system maintenance, they will notify the EDIT of scheduled maintenance in a reasonable time.
d. When special or emergency situations make it necessary to perform maintenance operations outside of the normal system operations schedule, these situations must be documented, management must be notified, and the operation processes used must be recorded.
e. Agencies shall develop change control procedures to accommodate resources or events that require changes to system operations.
f. Changes to system baselines require effective communication to ensure that information systems maintain secure operations and avoid delays due to processing consumption and to minimize downtime due to unforeseen problems during such changes.
g. Change control procedures must be documented and followed during the scheduled maintenance windows and take into consideration the following:
    i. Periods of maximum and minimum workflow.
    ii. The approval and notification process.
    iii. Interfaces with other applications, systems or processes.
    iv. External agency and departmental interdependencies.
    v. Change categories, risk and type.
    vi. The change request process.
    vii. Rollback plans and the point of no return.
    viii. Modifications to change control procedures for special or emergency circumstances.
h. All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy.
i. Upon the completion of a baseline change, the audit change logs must be retained in accordance with the Information Technology logging specs as described by TCSG.

Systems to be Monitored and Patched

All software and hardware systems will be monitored and patched with the latest stable security and critical updates to ensure system stability and security. All systems are running software and firmware with the latest stable software and firmware patches. When possible, systems will be scanned with at least two vulnerability scanners or methods. The following is a list of systems to be monitored and patched. This list is not intended to be comprehensive, and all other networked devices should be patched when feasible.

a. Access control devices for doors
b. Application software
c. Backup appliances
d. Banner Student Information System
e. Cell phones, College-owned
f. Digital signage
g. Environmental controls hardware and software
h. Firewalls
i. HVAC Controls
j. IP KVM and KMM devices
k. Printers
l. Projectors
m. Server firmware – Cisco
n. Server firmware – Dell
o. Storage appliances
p. Switches
q. Networked UPSs & PDUs
r. VoIP, Video Conferencing & Collaboration
s. Video surveillance cameras and NVRs
t. VPN devices

u. Windows Server and Client Operating Systems
v. Wireless controllers and APs

Summary information can be found in the Maintenance Schedule Guidelines for IT Assets. Additional information regarding each of the systems can be found in the CPTC IT Maintenance Schedule shared calendar in Office 365. All devices that cannot be upgraded will be either patched to the greatest extent possible, replaced, or isolated by network infrastructure devices by means such as ACLs. Further, all schedules will be compliant with TCSG's IT System Maintenance Standards.

Managing and Maintaining Backup Power Generators and UPSs

CPTC systems whose requirements demand uninterrupted information processing during power outages shall deploy backup power generators. Due to the cost of implementing generators, only the main server room at main sites will be considered for a generator. At locations where a backup generator is installed (Waycross and Camden at this time), the College will observe the following requirements:

a. Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer maintenance requirements and has an adequate supply of fuel. This falls under the CPTC Facilities division.
b. Ensure the generator has the electrical and fuel capacity to sustain the power load required by supported equipment for a prolonged period of time. This falls under the CPTC Facilities division.
c. Ensure the generator and switch are tested according to the manufacturer's specifications. This falls under the CPTC Facilities division.
d. Since there is a delay between a power fault and the start of the generator, the backup generator is combined with an uninterruptible power supply (UPS) to protect critical information technology systems that demand high availability. Such a combination bridges the power gap between the loss of power and the power supply from the generator as well as supports an orderly shutdown if the generator fails. This minimizes the potential for equipment damage, data loss, and software corruption. The generator/UPS combination can also provide continuous business operations if the power is off or unreliable for an extended period of time.
e. Contingency plans will specify procedures to be followed in the event the backup generator fails.

Managing and Using Hardware Documentation

The college will develop and maintain additional documentation that details hardware placement and configuration, provides appropriate documentation such as lists, spreadsheets, databases, flowcharts, etc. in order to effectively manage their information assets.

a. CPTC shall retain user documentation and technical specifications of information technology hardware.
b. Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff.
c. This documentation must be encrypted when sending to approved recipients. Typically, this includes other College IT staff, TCSG IT staff, TCSG Enterprise Application Services Staff, the College President, and other qualified recipients specified by TCSG or the College ISA.
d. Printed documentation that is no longer needed will be shredded.
e. The College shall maintain a current inventory of information technology (IT) hardware and software assets in a formal hardware inventory/register. The preferred means is by way of software.

f. The Georgia Asset Tag ID will be configured into the proper field for each piece of equipment where possible to improve tracking and inventory of all assets with this capability.

Maintaining Hardware (On-Site or Off-Site Support)

a. The College will provide or arrange maintenance support for all equipment that is owned, leased or licensed. Alternately, the College IT department may coordinate with the College Facilities department for such maintenance.
b. The College must arrange support services through appropriate maintenance agreements or with qualified technical support staff. Equipment or software without current maintenance agreements and firmware upgrades should be either covered, replaced, or isolated when these are not possible.
c. Records of all maintenance activities will be maintained.
d. To maintain the reliability of databases, maintenance must be performed on the operating system of the system that hosts the databases, or there is a greater possibility that the database itself will fail.

Responsibility

The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented

Adopted: March 5, 2020
Revised: September 19, 2023