CPTC Procedure - Physical and Environmental Protection

Scope

The NIST 800-53 security publication as well as the Technical College System of Georgia (TCSG) policies and procedures are the foundation for information technology security for all colleges in the TCSG system. These policies and procedures establish a system-wide set of standards for information technology security to maximize the functionality, security, and interoperability of TCSG's distributed information technology assets and technologies. This procedure applies to all employees of CPTC, contractors, and all other entities that support the operation and assets of the College. All entities involved in the maintenance of information systems and supporting infrastructure are responsible for adhering to all components of this procedure.

Role	Definition
CPTC President and Cabinet-level staff	CPTC College president, vice presidents, executive directors, and Campus Police Chief are responsible for the support of the Risk Management Plan and process, the review and approval of risk assessments, and recommendations and reporting to the CPTC ISA/Executive Director of IT regarding mitigation actions have been or need to be taken.
CPTC Information Security Administrator (ISA)	The College ISA, TCSG appointed per college, is responsible for ensuring that physical and environmental risks are managed in compliance with the requirements specified by TCSG policies and procedures as well as NIST 800 part 54. This should be accomplished by collaborating with TCSG and CPTC entities. The ISA is responsible for maintaining the appropriate operational security controls required for physical and environmental protection.
Executive Director of Facilities and Campus Police Chief	The Executive Director of Facilities, the Campus Police Chief, and other designated organizational official(s) at management level, are responsible for site security and ensuring the facility is safe for occupancy, authorization credentials, keys, physical access devices, etc.
Third Parties	Third party service providers are responsible for providing physical and environmental security in accordance with this policy. CPTC staff sponsoring third party service providers are responsible for notifying said providers of TCSG and CPTC policies and procedures regarding physical and environmental protection.

PE-1 - Policy

All College information assets will meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls as well as related TCSG security policies and guidelines. This document addresses the procedures and standards implementing the family of Physical and Environmental Protection controls from the NIST SP 800-53 standards.

TCSG and GTA have adopted the physical and environmental protection security principles established in NIST SP 800-53, "Physical and Environmental Protection" control guidelines for this security domain. The "PE" designator identified in each control represents the NIST-

specified identifier for the Physical and Environmental Protection control family. Each of these corresponds to the similarly designated sections of the annual risk assessment.
The following subsections in this document outline the Physical and Environmental Protection controls requirements that the College will implement and maintain in order to protect the privacy and security of sensitive information and to prevent the unauthorized use or misuse of College, staff, or student data.

PE-2 – Physical Access Authorizations

Access to CPTC buildings, rooms, work areas, spaces, and structures that house information systems, equipment, and data will be limited to authorized personnel. The College will also restrict access to non-digital media. Access is restricted to authorized individuals who are required to abide by TCSG-defined or CPTC-defined security measures. Other examples of this equipment and media include paper documents, notes, USB thumb drives, external hard drives, computer files, tablets, or any other type of media or media access.

a. System or data owners at CPTC will develop access policies for authorized individuals as well as visitors to CPTC facilities.
b. Information contained, stored, or represented on storage or presentation media for data that requires restricted access will be used to assess the risk presented. The risk will be considered when selecting the appropriate type of storage or presentation media for the data.
c. System or data owners will document procedures for:
    i. All media in the system holding data that requires restricted access
    ii. determining which individuals are authorized to access the media
    iii. specific measures that will be taken to restrict access to that media
d. Authorization credentials such as restricted keys, badges, identification cards, and smart cards will be issued to everyone accessing a restricted area.
    i. Following the level of least privilege, the level of access provided to each individual will not exceed the level of access required to complete the individual's job responsibilities.
    ii. The level of access to data and media will be reviewed and approved before access is granted.
    iii. Keys, badges, access cards, and combinations that can access restricted areas will only be issued to personnel who require access for a job-related function.
    iv. Rooms containing restricted media or systems should not be protected by doors using keys such as building masters or grand masters when assignment of high-access keys such as these grant access to other restricted systems that assignees should not have for the performance of their job duties.
    v. Employees are encouraged to display either an employee name badge or a State Identification Card.
    vi. Keys, combinations, and other physical access devices will be secured at all times to prevent unauthorized access to CPTC facilities and assets. These devices will be inventoried annually during the complete inventory check that occurs each year. Key inventory and control is under the control of the Campus Police Chief.
    vii. Employee's supervisors will fill out a Key Request Form for any key or security/alarm system codes.
    viii. The unauthorized duplication of keys is prohibited. All requests for duplicate keys will be submitted to the Campus Police Chief for review, approval and fulfillment. *Note: There may be a fee assessed to replace lost keys.*
    ix. Keys or access cards that are assigned to employees that open CPTC doors, locks, cabinets, desks, etc. will be turned in by the employee upon termination of

employment or transfer to another position that does not require restricted access.

x. Authorizations and access requirements and restrictions will be coordinated with system or data owners and the Campus Police Chief as required or needed.

e. Access lists and authorization credentials for medium and high sensitivity restricted areas will be reviewed and approved annually to ensure that:
    i. Access to restricted areas will be limited to only authorized personnel
    ii. The level of access provided to each individual will be consistent with the individual's job responsibilities
    iii. Access rights will be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides
f. Enforce physical access authorizations to the information system/media in addition to the physical access controls for the facility at spaces where restricted or highly restricted data is received, processed, stored, or transmitted.

PE-3 – Physical Access Control

CPTC data and system owners will carefully evaluate sites and facilities housing IT equipment for which they are responsible to identify and implement suitable controls to protect staff, data, and resources from environmental threats, physical intrusion and other hazards and threats.

a. The College will safeguard all sites, buildings and locations housing its IT assets.
b. All locations that house restricted or highly restricted data will be designed and secured in accordance the information being protected.
c. Physical access devices (e.g., keys, locks, combinations, card readers) and/or guards must be used to control entry to facilities containing information systems.
   These devices or guards are positioned at entry and exit points to rooms where IT systems that receive, process, store, or transmit restricted data reside will be enforced by the following:
    i. Verifying individual access authorizations before granting access to the facility.
    ii. Controlling ingress/egress to the room or structure using physical access control systems/devices or guards.
    iii. Guards can be members of the Campus Police staff, CPTC administrative employees, or other CPTC employees who use the equipment and media to be protected. If guards are used and to be responsible for protecting restricted assets, they must be designated and notified.
    iv. Physical access devices must be functioning properly. These devices should be checked to ensure proper functionality, and maintenance must occur on the appropriate basis.
    v. Shared combinations and keys must be changed on a routine basis.
    vi. In addition, combinations and keys that protect restricted IT equipment and media must be changed immediately for reasons including when:
        - Keys are lost.
        - Combinations are compromised.
        - Individuals using combinations are transferred, terminated, or no longer need access.
        - There is a theft or security violation in the area being protected.
d. All equipment that stores, processes, or transmits sensitive or restricted information must be located in an appropriate locked rack, room, or enclosure. This includes server rooms and data rooms; these may also be called MDFs and IDFs. Other closets that house sensitive equipment, cables, or connections also fall under this classification.

e. Authorized individuals may include CPTC and TCSG employees with a reason to be in the room, contractors completing work for or on the IT infrastructure, and vendors who are working with the IT staff.
f. Physical access controls should include some form of visible identification such as a Driver License or some other picture identification such as an approved name badge or acceptable guest badge.
g. A log of physical access for all individuals to server rooms will be maintained including entry and exit dates and times. The information will be collected in a format that creates an audit trail.
h. CPTC will control the number of people who have physical access to areas housing sensitive infrastructure equipment to reduce the threats of theft, vandalism, data loss, and unauthorized system access. The College will consider the following measures to control and restrict access to computing facilities and allow access with these guidelines in mind.
    i. Only people with authorized purposes for being in the server rooms and data rooms will be permitted. All others will be restricted.
    ii. Instructions will be issued to visitors explaining security requirements and emergency procedures.
    iii. Visitors to restricted areas will be escorted and should wear visible identification that clearly draws attention to their restricted status.
    iv. Where appropriate, the College can store resources in lockable storage cabinets and closets where the physical security controls are sufficient to protect the equipment from theft.
    v. College employees may use lockable file cabinets to store restricted or highly restricted data such as paper documents and computer media in a manner that is commensurate with the information's classification status.
i. Video cameras and/or access control mechanisms will be used to monitor physical access to each area classified as restricted.
j. The use of personal cameras, video recorders and mobile computing devices may be restricted from high security locations to protect the information being stored. This is the responsibility of the system or data owner.
k. Facilities that will house restricted or highly restricted data will have access controlled by a combination of security measures such as these below. This is not an exhaustive list, so combinations including other appropriate measures may be considered acceptable.
    i. Locked doors, cabinets, or drawers
    ii. Tempered glass or bars for windows
    iii. Alarms
    iv. Walls of solid construction and extending from real ceiling to real floor where necessary)
    v. Doors opened by RFID (or other ID Card) and a PIN (Multifactor Authentication, MFA)
    vi. Video cameras
    vii. Staffed reception desk
    viii. Fire doors on a security perimeter will be equipped with alarms as well as devices that close the doors automatically.
l. All physical access control deficiencies must be addressed. They should be added to the risk assessment with measures taken to address the deficiencies.

PE-4 - Access Control for Transmission Medium

The College will control physical access to information system equipment and data cabling within its facilities.

a. Protective measures to control physical access to information system distribution and transmission lines will include the following:
    i. Data rooms and wiring closets should be kept locked with the door closed when not being occupied by authorized personnel.
    ii. Network jacks should be disconnected, disabled, or locked when they are not being used
    iii. Protection of cabling by conduit or cable trays. This extends beyond established server, data, and wiring rooms.
b. Publicly accessible network jacks in data centers will provide only Internet access by default, unless additional functionality is explicitly authorized.
c. Open wireless networks, if required, will provide only Internet access or access to publically-accessible resources.
d. Physical access to networking equipment and cabling will be restricted to authorized personnel. This is defined in the TCSG Information Security Standards (ISS).

PE-5 - Access Control for Output Devices

The College will control physical access to information system output devices, such as computer monitors (displaying sensitive or restricted information in a location viewable by non-authorized people), FAX machines, copiers and printers, to prevent unauthorized individuals from obtaining the output:

a. Enable security functionality on printers, copiers and FAX machines when technically possible that requires users to authenticate with the device via credentials, a PIN, or hardware token in order to access the device.
b. Control physical access to output devices by placing devices in controlled areas requiring authorized badges or keys.
c. Privacy screens will be used to control visibility of output on monitors. Monitors may also be re-positioned away from view by unauthorized users.
d. This control is optional for LOW risk information systems. Medium or high risk information systems may require higher levels of authorization.

PE-6 – Monitoring Physical Access

College employees will monitor physical access to information systems to detect and respond to physical security incidents.

a. Coordination between the IT leadership, Facilities leadership, the Campus Police Chief, HR and other departmental leadership will occur when responsibilities overlap.
b. Logs of physical access will be reviewed at least quarterly by the CPTC ISA for IT staff or the system/data owner or designee if not an IT asset. The designee will report any anomalies, and the ISA will be responsible for initiating action based on anomalies.
c. Investigations of apparent security violations or suspicious physical access activities will be conducted. Investigations and results of reviews will be coordinated with The College's incident response plan:
    i. Remedial actions identified as a result of investigations will be developed and implemented.
    ii. Incident investigations will follow the CPTC Incident Response Plan. This plan defines when a situation may be labeled an incident and TCSG notified. Note: Only TCSG can declare a situation an incident per the plan.
d. Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities will be part of the College ISA, the incident response plan, and TCSG.

PE-6 (1) – Monitoring Physical Access – Intrusion Alarms / Surveillance Equipment (Moderate Control) Physical intrusion alarms and surveillance equipment will be

installed and monitored. Automated mechanisms to recognize potential intrusions and initiate designated response actions should be employed where feasible. Also, for access to information systems determined to be moderate and high, visitors must be escorted, and visitor activity must be monitored.

PE-8 – Visitor Access Records

College employees responsible for systems and locations will actively monitor the security access logs of areas housing information technology equipment.

a. Visitors must sign access records/logs for College-owned computing facilities.
b. Visitor records or logs will address the following requirements:
    i. Name and organization of the person visiting
    ii. Signature of the visitor
    iii. Date and time of entry and departure
    iv. Purpose of visit
c. In high sensitivity locations, automated mechanisms such as video cameras will also be installed to support the visitor access records/logs.
d. Visitor access records for server rooms and data rooms will be maintained for the duration of Georgia's records retention policies. This should be five years.

PE-9 – Power Equipment and Cabling

It is the responsibility of all College employees to protect power equipment and cabling for information systems as well as the facilities housing them from damage and destruction.

a. Both power and communication lines should be protected.
b. IT leadership will select and order dual power supplies or other technology that may share power between devices for critical infrastructure equipment where feasible.
c. IT and Facilities staff will employ multiple, physically separate electric circuits to avoid a single point of failure in the power supply. This helps ensure that power continues to flow to critical infrastructure equipment in the event one of the circuit breakers is tripped, a cable is cut or current is otherwise interrupted.
d. CPTC IT staff will install equipment that will automatically control and correct voltage irregularities for critical system components. This helps ensure that clean power continues to flow to the equipment in the event voltage fluctuates to unacceptable levels that would cause damage to the information system component. The most common example of this is the use of a power strip on the lowest devices to an uninterruptable power supply (UPS) on critical infrastructure equipment.
e. This control is optional for LOW risk information systems.

PE-10 – Emergency Shutoff

The College will provide the capability to shut off power to the information systems or individual system components in emergency situations.

a. The College will install emergency power switches near emergency exits in critical equipment rooms rooms to facilitate rapid power down in case of an emergency. Currently, this would include the main server room in Waycross.
b. Coordination must occur with facilities personnel as needed or required.
c. Emergency shutoff switches should be located in locations that facilitate safe and easy access. Additional information regarding placement of emergency power shutoffs can be found in the NFPA 70 guidelines.
d. The locations for emergency power shutoffs must be marked with signage and documented.
e. All necessary personnel working in the area of the emergency shutoff switch must be informed of the emergency power shutoff locations, and they must be trained to operate them safely.
f. Emergency procedures must be readily available to relevant personnel.

g. The emergency power-off capability must be protected from accidental or unauthorized activation.

PE-11 – Emergency Power

The College will protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems will continue to perform in spite of and during power outages and electrical anomalies such as power loss, brownouts, and spikes.

a. The three major methods for providing continuous power are listed below.
    i. Multiple electric sources via separate circuits in conjunction with multiple power supplies to avoid a single point of failure in the power supply
    ii. Uninterruptible Power Supply (UPS)
    iii. Backup generator
b. The College will scrutinize the availability requirements for critical equipment and determine which combination of these three methods best meets the needs of the College.
c. The College will analyze the emergency power requirements for critical systems based on the following best practices:
    i. Use of a UPS will provide a clean power source during brownouts or surges. A UPS will enable systems without a generator to gracefully shut down. Note: The batteries in the UPS used by the College have uptimes ranging from 10 minutes to 120 minutes after a loss of power.
    ii. College leadership will prepare contingency plans that include procedures to follow if there is a power failure that will last longer than the UPS was sized to supply power after power loss. This information will be written into the CPTC Business Continuity Plan and the Disaster Recovery Plan.
    iii. Periodic inspections of UPS equipment to ensure that the equipment has the ability to sustain, for a predefined period, the power load of the systems and equipment it supports, and is serviced according to the manufacturer's specifications.
    iv. UPSs will be centrally monitored and managed where possible.
    v. UPSs will be configured to send an alert to IT and Facilities staff when power is lost for more than 1 minute or when there is a problem with the UPS itself.
    vi. IT and Facilities staff will coordinate to address power problems.
d. A backup generator will be used in addition to a UPS when requirements demand high availability and continuous processing in the event of a prolonged power failure. Using both a UPS and a generator supports an orderly shutdown if the generator fails or depletes its fuel supply. This minimizes the potential for service interruptions, equipment damage, and data loss. UPSs enable systems with a generator to have a continuous source of power until the generator starts and comes online after the power is switched from line power to generator power. When a backup generator is required, the College should ensure the following:
    i. Power consumption by the equipment in the protected area serviced by the generator should be periodically measured and compared to generator capacity to ensure the generator has the capacity to power the supported equipment.
    ii. Generator load considerations must be made before adding additional equipment to a generator protecting critical IT infrastructure equipment.
    iii. All generators will be started at least monthly to ensure that they will start as well as to charge the start-up batteries if applicable.
    iv. The generator will be serviced regularly in accordance with the manufacturer's specifications. Generators for CPTC's network are required every year during

hurricane season, so generators should be inspected prior to this period of highest use.

v. An adequate supply of fuel will be available to ensure that the generator can perform for a prolonged period. Long-term fuel sources such as natural gas from a pipeline is preferable to recharged/refilled sources such as a propane tank.

PE-12- Emergency Lighting

The College will provide emergency lighting in case of a main power failure.

a. Automatic emergency lights will activate during a power outage or disruption. These lights should cover emergency exits and evacuation routes within the facility. This is already required, installed, and checked in accordance with fire code.
b. The automatic emergency lighting systems will be tested annually by the CPTC Facilities staff or designees to ensure they are fully operational.
c. The results of the test will be documented.

PE-13 – Fire Protection

The College will have security controls in place that will assure the availability and continual service of critical IT systems. These include systems that alert, monitor, and log intrusions, fires, smoke, water, electrical effects, and electrical supply interferences. This control primarily applies to facilities containing critical information system infrastructure. Many of these requirements are already required, installed, and checked in accordance with fire code. Examples of greatest interest to IT infrastructure include data centers, server rooms, and network closets.

a. Fire extinguishers must be checked annually, and the date of inspection must be documented on the extinguisher.
b. All fire protection systems and tools must be tested in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.
c. The College will provide fire-resistant storage for documents and media containing mission critical information.
d. Important documents saved in a filing cabinet or other storage system that is not fire, smoke or water safe should have duplicate copies of the information stored in alternate locations. This may or may not include digital storage options due to limitations imposed by governing bodies.
e. Flammable materials such as paper, cardboard, etc. will not be stored in MDFs and IDFs.

PE-13 (3) – Fire Protection – Automatic Fire Suppression (Moderate and High Control)

a. The College will install and maintain fire detection and suppression systems designed for use in critical IT infrastructure locations.
b. Fire detection systems in critical IT infrastructure locations should activate automatically and notify emergency personnel and IT staff in the event of a fire. This gives protection to mission critical IT infrastructure when the facility is not staffed on a continuous basis.

PE-14 – Temperature and Humidity Controls

College IT and Facilities staff will implement and maintain automatic temperature and humidity controls in critical data and server rooms to prevent fluctuations potentially harmful to equipment.

a. College IT and Facilities staff will deploy and configure devices that continuously monitor temperature and humidity in restricted areas.

b. Monitoring systems and devices will provide an alarm or other notification when temperature and/or humidity are outside configured tolerances due to heating, ventilation or air conditioning (HVAC) failures. These failures may adversely affect critical IT assets.
c. Temperature and humidity must be maintained within limits as required by the equipment being protected.

PE-15 –Water Damage Protection

a. CPTC's primarily Facilities and IT leadership must design and include measures to prevent water damage to equipment in critical information infrastructure rooms and structures.
b. Rooms having critical information infrastructure must have water shutoff valves that can be used to protect equipment from damage resulting from water leakage.
c. These valves must be:
    i. accessible
    ii. working properly
    iii. marked with signage
    iv. known to key personnel

PE-16 – Delivery and Removal

Delivery areas should not be located in a place that endangers the information systems.

a. Information system components and packages that are delivered to or removed from IT server rooms will be authorized, monitored, and controlled.
b. Delivery personnel should be accompanied by an authorized CPTC or TCSG employee.
c. Records of items entering and exiting the IT server rooms will be recorded in the attendance logs.

PE-17 – Alternate Work Site

The College will provide available alternate work locations such as offices at other CPTC campuses or sites, employee homes (Work From Home, WFH), or other suitable locations as part of contingency operations.

a. The security controls at alternate work sites will be assessed, as feasible. Alternate work sites will be equipped with equipment needed to resume temporary operations, even if minimally. Employees will communicate with IT staff responsible for security in case of security incidents or problems. That designee for CPTC is the Information Security Administrator (ISA) appointed by TCSG, the Executive Director of IT.
b. CPTC employees must take reasonable steps to protect equipment and media, both digital and non-digital, from damage and unauthorized access.
c. CPTC employees will secure and protect communications with restricted information and equipment while working at off-site locations. The NIST 800 component, Access Control Policy, Section AC-17 – Remote Access, describes and defines remote access security requirements.
d. Alternate work sites must meet security control requirements at all levels – federal, Georgia, and TCSG.
e. If The College does not have direct control over the remote location, The College will enter into a contract with the owner of the remote location that stipulates the access controls and protection that the owner will implement. The following controls will be negotiated and implemented for alternate work sites.
    i. Physical security and access to the College's IT infrastructure.
    ii. Acceptable environmental design requirements for secure data storage (i.e., fire suppression and detection equipment, heating, ventilation, and air conditioning [HVAC], measures to prevent water damage, etc.).

iii. College equipment that is being used or stored at an alternate work site must be secured when not in use. Examples of alternate work sites would be an employee's home, a conference, a hotel, home, or other alternate site.
iv. College equipment transported in vehicles must not be openly visible. It should be stored in the trunk, under a blanket, or in another hidden way.
v. College equipment must not be stored in vehicles overnight.
vi. NIST SP 800-46, Revision 1 must be used as guidance for security in telework and remote access.

f. This control is optional for LOW-risk information systems.

PE-18 – Location of Information System Components

The College must designate and design locations for critical IT components within the facility to minimize the potential for damage from physical and environmental hazards as well as to minimize opportunities for unauthorized access.

a. The location or site for critical IT infrastructure and media must be considered with regard to physical and environmental hazards.
b. Physical and environmental hazards include, but are not limited to, hurricanes, flooding, fire, tornados, smoke, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation.
c. If water pipes are running overhead, then cabling or equipment should not be placed underneath the pipes.
d. The location or site of the facility where the information system resides must be planned with regard to physical and environmental hazards.
e. For existing facilities, the physical and environmental hazards must be considered in the risk mitigation strategy for the information system.
f. This control is optional for LOW-risk information systems.

Responsibility

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

Adopted: January 19, 2021
Revised: September 19, 2023