Queens College Technology Standard	No: QC-ITS-Security-023
Physical and Environmental Protection Standard	**Updated: 09/08/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

To ensure that Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope – College-Wide

This is a college-wide standard and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This policy is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This standard encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

1. PHYSICAL ACCESS AUTHORIZATIONS
   a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.

b. Issue authorization credentials for secure area access.
c. Review the access list detailing authorized secure area access by individuals and remove individuals from the secure area access list when access is no longer required.

2. PHYSICAL ACCESS CONTROL
   a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the secure areas.
   b. Control ingress/egress to the secure areas using defined physical access control systems/devices.
   c. Maintain physical access audit logs for defined entry/exit points.
   d. Provide defined security safeguards to control access to areas within the secure areas officially designated as publicly accessible.
   e. Escort visitors and monitors visitor activity in secure areas.
   f. Secure keys, combinations, and other physical access devices.
   g. Inventory keys to designated secure areas every year.
   h. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.
3. SECURE AREAS PENETRATION TESTING
   a. Employ a penetration testing process that includes unannounced attempts to bypass or circumvent security controls associated with physical access points to the secure areas as determined by the CISO's Office.
4. ACCESS CONTROL FOR TRANSMISSION MEDIUM
   a. Control physical access to networking rooms within entity facilities using appropriate security safeguards.
5. ACCESS CONTROL FOR OUTPUT DEVICES
   a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
   Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

6. MONITORING PHYSICAL ACCESS
   a. Monitor physical access to the secure areas where the information system resides to detect and respond to physical security incidents.
   b. Review physical access logs as needed and upon occurrence of [entity defined events or potential indications of events]; and coordinate results of reviews and investigations with the organizational incident response capability.
7. VISITOR ACCESS RECORDS

a. Maintain visitor access records to the secure areas where the information system resides for a minimum of 1 year; and reviews visitor access records monthly.

8. POWER EQUIPMENT AND CABLING
    a. Protect power equipment and power cabling for the information system from damage and destruction.
    b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.
9. EMERGENCY SHUTOFF
    a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.
    b. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.
10. EMERGENCY POWER
    a. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.
    b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

11. EMERGENCY LIGHTING
    a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the secure areas.
    b. Provide emergency lighting for all areas within the secure areas supporting essential missions and business functions.
12. FIRE PROTECTION
    a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

13. TEMPERATURE AND HUMIDITY CONTROLS
    a. Maintain temperature and humidity levels within the secure areas where the information system resides at appropriate levels.
    b. Monitor temperature and humidity levels regularly to include alarms or notifications of changes potentially harmful to personnel or equipment.
14. WATER DAMAGE PROTECTION
    a. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
       This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

15. DELIVERY AND REMOVAL
    a. Authorize, monitor, and control entering and exiting the secure areas and maintain records of those items delivered and removed from secure areas.
       Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

16. ALTERNATE WORK SITE
    a. Employ equivalent controls at alternate work sites.
    b. Assess as feasible, the effectiveness of security controls at alternate work sites.
    c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.
       Alternate work sites may include, for example, other facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	**Description of Change**	**Reviewer**
9/20/22	Initial changes to apply to Queens College	DVogel
07/18/2023	More Changes to apply to Queens College	DVogel
09/08/2023	Added #10, Converted to Standard, Aligned to Gartner Recommendations.	DVogel

9.0 Related Documents

10.0 External Documents