



Office of Information Technology

IT Process
OFFICE OF INFORMATION TECHNOLOGY
NETWORK OPERATIONS CENTER
PHYSICAL ACCESS

Process: IT15001B
Original Effective Date: 11/30/2009
Last Revised: 3/24/2022

Last Reviewed: 3/24/2022
Next Scheduled Review Date: 04/01/2025

Version #: 2.1
Administrative Owner: Chief Technology Officer

PURPOSE

The purpose of this process is to define the criteria by which the Office of Information Technology (OIT) Network Operations Center (NOC) physical access privileges are granted in accordance with the OIT Facility Physical Access Standard.

SCOPE

This process applies to all OIT employees, contractors, and vendors and all visitors to the NOC. The NOC is located on the Takoma/Park Silver Spring (TPSS) Campus of Montgomery College within the Information Technology Operations Center (ITOC).

DEFINITIONS

Table with 2 columns: Term, Definition. Rows include Access Card, Contractor or OIT Contractor, Emergency, Level A Access Privileges - Escorted Access, and Level B Access Privileges - Unescorted Access.

	<ol style="list-style-type: none"> 3. Once admitted to the NOC Server Room, the individual may work without escort and may serve as an escort for Level A access. 4. Both the individual and their escort must assure compliance to NOC access and operational regulations. 5. During unmanned hours or emergency situations, NOC personnel and/or TPSS Campus Security personnel will be available to provide Level C access support.
Level C Access Privileges – Authorized Access	<ol style="list-style-type: none"> 1. The individual has assigned facility access privileges to enter the NOC and move freely within the NOC without escort. 2. The individual must assure compliance to NOC access and operational regulations. 3. Non-OIT Level C Authorized Access is limited to the TPSS Campus Security Lead Officer on duty. This access privilege is to be used for emergency purposes only.
Monitoring Area	The area from which NOC personnel monitor Server Room activity.
NOC Personnel	An individual who is assigned to the Montgomery College OIT NOC. These individuals may be Montgomery College employees or contractors hired by OIT.
OIT personnel	An individual who is assigned to the Montgomery College OIT. These individuals may be Montgomery College employees or contractors hired by OIT.
Vendor	An external business entity contracted by Montgomery College for a set period of time for the purpose of providing a service or delivering a product.
Visitor	Anyone who has not been awarded Authorized or Unescorted Access privileges to the NOC.

PROCESS

A. GENERAL

1. The NOC is operational 24/7 and manned 24/7 except for Friday night from 10:00pm to Saturday morning 8:00am, Saturday night from 6:00pm to Sunday morning 8:00am, and Sunday night from 6:00pm to 9:00pm. The NOC is not manned on College holidays and other days the College is officially closed.
 2. Montgomery College employees, contractors, and vendors with physical access privileges to this OIT governed facility have the responsibility to abide by the requirements as outlined in this document. They must also comply with existing College policies and procedures and Information Technology (IT) standards, processes, and procedures, and protect College academic and administrative information when accessing College technology resources.
 3. Montgomery College employees and OIT contractors are assigned access privileges to the NOC if their normal College business duties require routine and recurring access to areas within the NOC. Non-NOC resident access is limited to areas where business is conducted relative to the individual's specific role and responsibilities.
 4. Periodic auditing of assigned NOC access privileges is performed by the NOC Manager for compliance to access regulations. Periodic auditing of NOC access records is performed by the NOC Manager with approval of the IT Policy Administrator (ITPA).
-

5. In addition to access card and surveillance monitoring, an activity logging system is utilized in the NOC. Use of the logging system is detailed in the NOC Access Log Procedure.
6. Montgomery College OIT employees must wear their Montgomery College ID card as their personnel ID badge and OIT contractors must wear their Montgomery College Contractor ID card as their personnel ID badge while on duty.
7. Upon arrival at the ITOC, all non-OIT personnel must sign a visitor log before proceeding into the NOC. Visitor ID badges and visitor access cards will not be issued.
8. Video surveillance equipment may be used in the NOC. The surveillance system exists for the purpose of protecting information assets of the College and not for the purpose of protecting personal property or providing personal safety. Surveillance equipment is limited to public or secured areas where individuals do not have a reasonable expectation of privacy. Surveillance is executed in accordance to Federal and State legal requirements, College Policy and Procedure, and as approved by the Chief Information Officer (CIO) and Chief Facilities Officer (CFO). Specifically, video cameras monitor entrances to office areas and to IT asset areas as appropriate. A retention policy for how long surveillance data will minimally be available shall be part of the procedures for video surveillance. Requests for access to content stored in a surveillance system must be approved by the IT Policy Administrator (ITPA).
9. Applications for Level C access privileges at the NOC or exceptions to this process are approved by the NOC Manager or in his absence, the Chief Technology Officer (CTO).
10. Requests for information regarding Montgomery College NOC internal operational procedures should be directed to the NOC Manager.

B. NOC SERVER ROOM ACCESS

1. Server Room Access

- a) An activity logging system is utilized to identify individuals entering and exiting the Server Room. Use of the logging system is mandatory and detailed in the NOC Access Log Procedure.
- b) Access to the Server Room is limited to individuals with Level C access privileges.
- c) Individuals with Level B access privileges may only be let into the server room by individuals with Level C access privileges.
- d) Individuals with Level A access privileges may only be let into the server room by individuals with Level C access privileges. Once inside they must be escorted by individuals with Level C or Level B access privileges.
- e) TPSS Campus assigned janitorial services are assigned Level A access privileges to the Server Room and must complete their work responsibilities while NOC personnel are on duty.

2. Server Room Rear Door Usage

- a) The Server Room Rear Door must ONLY be used when the NOC is receiving delivery of large items that cannot be received through the Server Room Front Door.
- b) The Server Room Rear Door is to be opened ONLY from the inside except in an emergency situation. Before opening the door, the TPSS Security Office (x71600) must be notified using a telephone from the NOC Monitoring Area.
- c) Each use of the Server Room Rear Door must be clearly documented as detailed in the NOC Access Log Procedure.

- d) Individuals with Level C access privileges must use their assigned access card to log their action each time they open the Server Room Rear Door. This will notify TPSS Campus Security that the door is in use. The TPSS Campus Security Office will confirm that an approved access card was used. Failure to follow this step will result in a TPSS Campus Security Office response.

EXCEPTIONS

Exceptions to this process will be considered on a case by case basis in accordance with the IT Exceptions Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, vendor or other agent found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

- ◆ Gramm-Leach-Bliley Act (Nov 1999)
- ◆ Montgomery College Policy 66001, Acceptable Use of Technology
- ◆ Montgomery College Safety and Security Policy (77001)
- ◆ OIT Facility Physical Access Standard

WEB SITE ADDRESS FOR THIS PROCESS

https://info.montgomerycollege.edu/offices/information-technology/it-security/it_standards.html

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
November 30, 2009	Original roll-out of this NOC Physical Access document.	Patrick Feehan, Information Security and Privacy Director/ITPA
November 30, 2015	Revised. (Version 2.0)	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates. (Version 2.1)	Nell Feldman / Keith Wilson
March 2022	Reviewed. (Minor clarification changes. Updated Administrative Owner. Added Website Address of the process	Nell Feldman, Interim Director of Information Security Services/CISO/IT Policy Administrator

