



OIT 62.010: Data Centers Security

Responsible Executive: Chief Information Officer (CIO)
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: May 14, 2008
Effective Date: May 14, 2008
Revision Date: December 17, 2009

Policy Statement

Norfolk State University (NSU) Office of Information Technology maintains secured spaces to protect the critical information systems. The Physical & Environmental Security Policy governs how and to whom access to OIT secured spaces is granted, and the environmental conditions to be maintained within the secure areas described below and located in the Bowser Building and the McDemmond Center.

Purpose

This policy establishes procedures for physically securing OIT spaces and maintaining appropriate environmental conditions for the data centers, network operation and security center (NOSC), storage room, cage and tape backup library.

Responsibilities

The Office of Information Technology (OIT) is responsible for physically and environmentally securing the equipment under its care.

General OIT Spaces:

The OIT Office suite is to be electronically monitored 24x7 via cameras. Access is to be controlled and logged via the University's Stanley Best (SpartanCard) door security system. OIT associates will have access via the SpartanCard system. Non-OIT NSU associates must identify themselves at the front desk before being allowed to pass in order to conduct daily business. Non-NSU personnel are to be signed in and the OIT staff being visited must escort them.

High Security Spaces:

Data Centers/Server Rooms

These procedures are set for maintaining security of the data center.

- Doors will remain secured at all times. This is to limit access, maintain temperature, and to ensure the correct operation of the fire suppression system.
- Access is electronically monitored 24x7 via cameras and the SpartanCard access system.
- All work by vendors must be conducted in the Network, Operations, and Security Center whenever possible. Team Leads must approve any exceptions to this.
- All visitors and vendors entering the secure areas must sign the access log located at the NOSC door and must be escorted at all times.
- Physical Keyboard, Video, Mouse (KVM) devices are to be kept in controlled spaces. Logical (IP based) KVM must be secured via password. Access to the physical or logical KVM will be restricted to those who need KVM access.

SpartanCard access is granted on an “as needed” basis only. The Chief Information Officer (CIO) is the person responsible for granting or denying access. When a person leaves OIT and/or the University, their SpartanCard access to OIT spaces will be promptly terminated. The following guidelines will be followed when determining if access should be granted:

Must be members of the Norfolk State University Office of Information Technology; and

- Must need access on a regular basis (more than once a month); and
- Must need to physically access the system hardware for the purpose of changing tapes, moving cables, etc; or
- Must be direct supervisors of the individuals who work on system hardware.

In addition, SpartanCard access to the Data Center may be granted to members of the NSU Police Department, Security and Facilities Management for the purpose of monitoring and responding to Data Center physical and environmental emergencies.

Rules while in the Data Centers:

- No food or drink is allowed within the data centers.
- No Hazardous materials are allowed within the data centers.
- All packing material when possible must be removed from computer equipment/components in specified staging areas before being moved into the data centers. This includes cardboard, paper wrap, plastic, wood and other such materials.
- No cleaning supplies are allowed within the data centers without prior approval. This includes water.
- No cutting of any material (pipes, floor tiles, etc...) shall be performed inside the data centers unless special arrangements are made in advanced.
- Boxes, tapes, CD's and other material shall not be stored inside the data centers.
- OIT employees shall only access racks that contain equipment for which they are personally responsible.
- Only Data Center staff shall access the sub-floor or remove tile.

- ID must be worn and visible at all times.
- Communicate all problems to data centers staff.
- In the event of an emergency notify data centers staff immediately

Environmental Security:

Appropriate environmental conditions must be maintained within the server rooms for the operation of electronic systems. These conditions include:

- Input Temperature <72 degree F
- Humidity 20% - 60%

The data center operations manager will perform frequent checks of the data centers to ensure these environmental conditions are maintained. An automatic alert system notifies the appropriate IT staff if the environmental conditions fall outside the preset limits. If at any time the ambient temperature exceeds 80 degree F, emergency cooling (with the assistance from Facilities Management portable HAVC systems will be obtained from university contracted vendors) would be utilized so a limited or full server room shutdown would not be required.

The data centers are equipped with an automatic FM-200 clean agent fire suppression system, uninterruptible power supply (UPS), and backup generators.

Tours and Visitors:

Tours and visitors shall only be allowed to view secure spaces such as the Data Center, NOS and the Tape Library from the hall through the glass window.

Other Secure Spaces

OIT operates spaces other than the server rooms for the monitoring of systems operations or storing of IT equipment. Access to these spaces is to be monitored 24x7 via SpartanCard access and/or cameras. These spaces are the Storage Room, and High Security Cage.

- MCAR OIT Storage Room – Storage area for storing unused equipment, IT or otherwise.
- MCAR OIT High Security Cage – Fenced area within the OIT storage room for storing high value.

SpartanCard access is granted on an “as needed” basis only. The Chief Information Officer (CIO) and/or the Director of Enterprise Information Systems are responsible for granting or denying access. When a person leaves OIT and/or the University, their SpartanCard access to OIT spaces will be promptly terminated. The following guidelines will be followed when determining if access should be granted:

- Must be members of the Norfolk State University Office of Information Technology; and
Must need access on a regular basis (more than once a month); or
- Direct supervisors of the individuals who require access can also be given access.

Only the Operations Manager and the Chief Information Officer (CIO) or their designee will have access to the high security cage.

Emergency Evacuation Procedures:

McDemmond Center Data Center and Other OIT MCAR Areas

In case of an Emergency Evacuation (due to fire, biohazard, etc), all personnel will exit the Center using the stairwells at both ends; no one is to use building elevators during emergency evacuations.

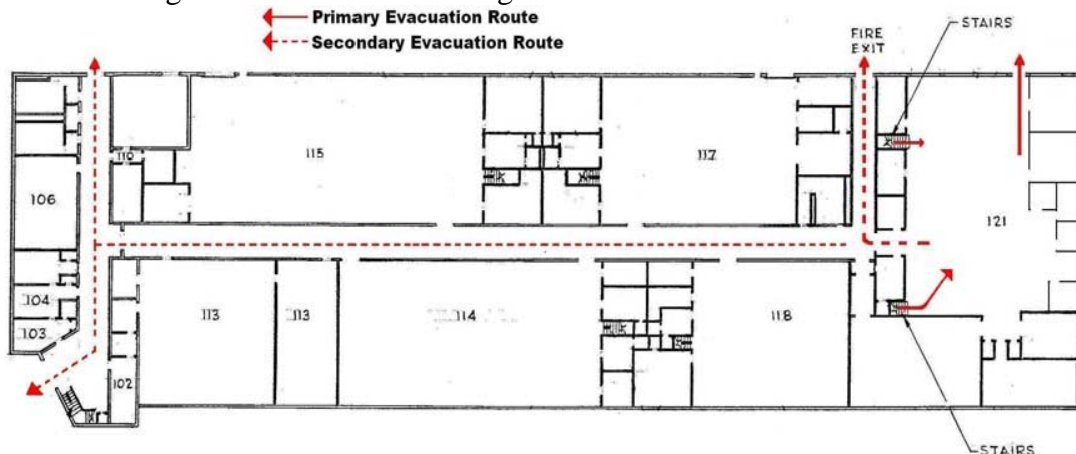
Once outside the Center, OIT personnel and any visitors will assemble in the rear of the parking lot at a safe distance from the building and out of the way from any emergency response personnel. All personnel will remain at the designated assembly point and not leave until authorized by emergency personnel.

Doors to secured areas, if open, should be closed during evacuation. The data center operations manager or his/her designee will do a quick sweep of the Data Center to insure it is secure.

Upon approval by emergency personnel and before reentry by OIT staff, the data center operations manager or his/her designee will re-enter the OIT space and inspect the secure spaces to insure they were not compromised.

Bowser Building Data Center

The Bowser Data Center is a remote facility but personnel do enter it regularly to perform system tasks and inspections. In case of an Emergency Evacuation (due to fire, bio hazard, etc), the following routes out of the building will be followed.



Once outside the Bowser Building, OIT associates will assemble in the field between Bowser and the Library. All personnel will remain at the designated assembly point and not leave until authorized by emergency personnel.

Doors to secured areas, if open, should be closed during evacuation.

MCAR drawing to be inserted below:

