



OIT 62.702: Facilities Security

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for University electronic information against damage, theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

II. Purpose

The Facilities Security policy identifies the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, and personnel.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

NSU shall or shall require that its service provider document and implement facilities security practices. At a minimum, these practices must include the following components:

1. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).
2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.
3. Require appropriate environmental controls such as electric power, heating, fire suppression, humidity control, ventilation, air-conditioning and air purification, as required by the IT systems and data.
4. Protect against physical access by unauthorized personnel.

5. Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.
6. Provide a system of monitoring and auditing physical access to sensitive IT systems.
7. Require that the ISO or designee periodically review the list of persons allowed physical access to sensitive IT systems.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.