



OIT 62.805: Access Determination and Control

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

Access Determination and Control reduces risk to University information by specifying access determination and control requirements that restrict access to information to only individuals who require such access as part of their job duties.

II. Purpose

The Access Determination and Control policy identifies the steps necessary to restrict access to IT systems and data to authorized individuals.

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 access determination and control practices for all sensitive agency IT systems and all third-party IT systems with which sensitive University IT systems interconnect. At a minimum, these practices shall include the following components:

1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.

Note: NSU should consult the Code of Virginia § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.

2. Restrict visitor access from facility areas that house sensitive IT systems or data.
3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.

4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Policy 62.502 and Policy 62.702.
5. Establish termination and transfer practices that require return of University logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.
6. Temporarily disable physical and logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.
8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the University prohibit a complete separation of duties.

Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.
9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.

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.