Standard Title: Access Control
Standard Number: IS-S702
Responsible Office: Information Security Office

Although students, faculty, staff and others require access to *university resources* for academic and business purposes, access must be limited to what is specifically authorized. Use of *university resources* beyond that level exposes them to unnecessary risk with no corresponding academic or business value. This standard establishes requirements regarding access to *university resources* as well as the responsibilities for stewardship of *university resources*. As stated in the Information Security Terms Guideline (IS-G100), "*university resources*" refer to *data* in any form and recorded in any manner and computer-related resources operated, owned or leased by the *university*, including but not limited to:

- *Networks* and n*etwork* appliances
- Computers (*servers*, workstations and laptops)
- Printers
- Software and applications
- Thumbdrives, printouts and paper, etc.
- Any other computer-related equipment, *device* or hardware used to access, store, transmit or interface with another *university resource*

Minimum Standards

1. Access Control

Physical and logical access to *university resources* must be controlled. The level of control will depend on the level of risk associated with loss or *compromise* of *university resources*.

Violations of this standard should be reported to individuals authorized to grant access to *university resources* or to the Office of Information Security.

2. Physical Access Control

The level of physical access control for any area that houses *university resources* must be commensurate with the level of risk associated with their loss or *compromise*.

All *devices, including mobile devices,* on which *confidential university data* are stored must be kept in a physically secure location when the user or other responsible individual is not present.

3. Logical Access Control

University information shall be used only for appropriate *university* purposes.

University information may not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her *university* position or affiliation.

Those authorized to access *university* information are responsible for properly securing it from unauthorized access, as well as for securing and protecting passwords, keys and other forms of access control.

As stated in the Minimum Security for Networked Devices Standard (IS-S602), all users must be assigned a unique identifier, such as UA NetID, for identifying and tracking user identity. Group *accounts* are discouraged, but if used, they must be affiliated with a responsible individual.

Those authorized to grant or revoke access to *university* information must:

- document procedures to ensure that access is appropriately assigned, modified as needed, and canceled promptly when individuals transfer to other positions or leave the *university*, and that access privileges and their implementation are reviewed periodically, at least annually; and

- ensure that *university resources* under their responsibility have adequate features and controls to support the proper management of user access.

Those accepting custody of confidential *data* on behalf of the *university* (e.g., for clinical trials, healthcare related activities, export controlled projects or through contractual outsourcing) must ensure that the information security requirements related to the acceptance of that confidential *data* are met.

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Related Guidance
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Data Classification Standard (IS-S302)
Data Facility Physical Security Standard (IS-S501)
Management Responsibilities for Information Security Standard (IS-S400)
Minimum Security for Networked Devices Standard (IS-S602)

Revision History

Initial Draft	11/29/07
Effective Date	7/1/08
Revised Draft	9/17/12
Effective Date	11/1/12