

**Old Dominion University  
Technology Policies, Standards, Procedures and Guidelines**

**IT Access Control Policy**

**Title:** IT Access Control Policy  
**Reference Number:** Policy 3501

**Purpose**

Access to Old Dominion University computing resources is granted in a manner that carefully balances restrictions designed to prevent unauthorized access against the need to provide unhindered access to informational assets.

**Access Control**

The University will provide all employees and other users with the information they need in order to carry out their responsibilities in as effective and efficient manner as possible.

Access to private information will be limited to authorized persons whose job responsibilities require it, as determined by an appropriate approval process, and to those authorized to have access by state or federal law.

Access is given through the establishment of a unique account in accordance with account request procedures. Exceptions to this policy include stand-alone personal computers, public access computers or related resources, and those student labs where individual student accounts are not required.

Users are expected to become familiar with and abide by University policies, standards and guidelines for appropriate and acceptable usage of the networks and systems. All users will have access to expectations, knowledge, and skills related to information security.

Every user must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent. Users electing to place information on digital media or storage devices or maintaining a separate database are responsible for ensuring that security, confidentiality, and integrity are maintained in accord with this policy.

Users are obligated to report instances of non-compliance.

**Definitions**

**Access** is defined as the ability and means necessary to store data in, to retrieve data from, to communicate with, or to make use of any resource of a system.

**Authorized Persons** are defined as people who have established a need and received the necessary authorization. Persons must be a member of the University's administration, faculty, or staff; registered students; or other individuals sponsored by the University.

**Information Technology Resources** are defined as computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services. It is in the interest of the Commonwealth and Old Dominion University that Virginia is in the forefront of developments in technology. For that reason, this standard shall not be construed to hamper the pursuit of the mission of the institution in instruction and research.

**Old Dominion University  
Technology Policies, Standards, Procedures and Guidelines**

**Policy References**

**ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.**

Ⓢ Policy Foundation:	Federal and State Law Policy 3500 Use of Computing Resources Policy 3503 IT Regulatory Compliance Policy Policy 3505 IT Security Policy
📄 Related Standards:	Acceptable Use Standard Security Awareness Standard Disciplinary Action
📄 Related Procedures, Forms:	Computer Account Request Form Reporting Violations
① Related Guidelines:	ISO Reference 05.02.01 Commonwealth Security Policy
✂ Maintenance:	Office of Computing and Communications Services
✓ Effective Date:	Reviewed on an annual basis
✓ Approved by: January, 2006	Rusty Waterfield Acting Assistant Vice President, Office of Computing and Communications Services
✓ Approved: January, 2006	University Advisory Council on Technology <input checked="" type="checkbox"/> Required for Standard
✓ Approved: October 1, 2007	Roseann Runte, President <input checked="" type="checkbox"/> Required for Policy