OLD DOMINION UNIVERSITY
University Policy

Policy #3501
INFORMATION TECHNOLOGY ACCESS CONTROL POLICY

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: February 21, 2011

A. PURPOSE

The purpose of this policy is to outline the manner in which access to Old Dominion University information technology (IT) resources is granted.

B. AUTHORITY

Virginia Code Section 23-9.2:3, as amended, grants authority to the Board of Visitors to establish rules and regulations for the institution. Section 6.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Restructured Higher Education Financial and Administrative Operations Act, Virginia Code Section § 23-38.88, as amended

C. DEFINITIONS

Access – The ability and means necessary to store data in, retrieve data from, communicate with, or make use of any resource of a system.

Authorized Persons - Individuals who have established a need and received the necessary authorization to access information technology resources.

Data - An information asset that represents, but is not limited to, individual data elements, lists, addresses, documents, images, measurement samples, programs, program source code, voice recordings, aggregations of data, or other information in a digital format. Data in a tangible object, typically paper, is excluded from this policy, but is subject to other University policies, including, but not limited to, policies on records management and confidentiality.

Information Security Officer (ISO) – The Old Dominion University employee, appointed by the President or designee, who is responsible for developing and managing Old Dominion University's IT security program.

Information Technology Resources – Include, but are not limited to, computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

User - Includes anyone who accesses and uses Old Dominion University information technology resources.

D. SCOPE

This policy applies to all users of Old Dominion University information technology resources and governs all information technology resources whether owned by or operated for University business through contractual arrangements, including, but not limited to, all employees, students, volunteers, employees of affiliated organizations, and visitors to the institution. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons attending classes whether enrolled or not enrolled. Affiliated organizations are separate entities that exist for the benefit of the University and include the Foundations, the Community Development Corporation, and the Alumni Association. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests and all other persons located on property, owned, leased, or otherwise controlled by the University.

E. POLICY STATEMENT

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 data will be limited to authorized individuals whose job responsibilities require it, as determined by an approval process, and to those authorized to have access by Federal, or State laws or in accordance with University policies and standards. The process for requesting, granting, administering, and terminating accounts, on IT systems, including accounts used by vendors and third parties, are provided in the Account Management Standard 05.2.2.

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

All users of IT systems are responsible for reading and complying with University information technology requirements, reporting breaches of IT security, actual or suspected, to University management and/or the Information Security Officer, taking reasonable and prudent steps to protect the security of IT systems and data to which they have access, and complying with any Federal, State, or local statutes and University policies and standards as might apply to these resources. Every user must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent.

Old Dominion University reserves the right to revoke any user's access privileges at any time for violations of policy, standards and/or conduct that disrupts the normal operation of information technology resources.

F. PROCEDURES

The specific procedures, standards, and guidelines to be utilized for compliance with this policy are published on the Office of Computing and Communications Services IT Policies website and links to these documents are listed herein.

OCCS Standard 01.4 - Disciplinary Action
OCCS Standard 02.4.1 - Data Classification
OCCS Standard 02.6.2 - Risk Assessment
OCCS Standard 05.2.2 - Account Management
OCCS Standard 05.4.1 - Remote Access
OCCS Standard 05.4.2 - Portable Computer Management
OCCS Standard 05.4.3 - Third Party Access
OCCS Standard 05.4.4 - Virtual Private Network
OCCS Standard 06.2.1 - Digital Media
OCCS Standard 06.2.2 - Data Storage Media Protection
OCCS Standard 08.2.2 - Access Determination and Control
OCCS Standard 08.2.3 - Payment Gateway Access
OCCS Standard 08.4.2 - Acceptable Use
OCCS Standard 08.4.3 - Residential Network

G. RESPONSIBLE OFFICER

Assistant Vice President for Computing and Communications Services

H. RELATED INFORMATION

Old Dominion University Board of Visitors Policy 1626 - Information Technology Management

POLICY HISTORY
****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Rusty Waterfield — February 21, 2011
Responsible Officer Signature — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks — October 28, 2010
Policy Review Committee (PRC), Chair Signature — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Robert L. Fenning — January 20, 2011
Responsible Oversight Executive Signature — Date

University Counsel Approval to Proceed:

/s/ James D. Wright — February 10, 2011
University Counsel — Date

Presidential Approval:

/s/ John R. Broderick — February 21, 2011
President — Date

Policy Revision Dates: October 1, 2007; February 21, 2011

Scheduled Review Date: February 21, 2016