A. PURPOSE

The purpose of this policy is to state the codes of practice with which the University aligns its information technology security program and documents the best practices and standards with which the University aligns its security activities.

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.

Virginia Code Section 23-38.88, as amended, Eligibility for Restructured Financial and Administrative Operational Authority.

C. DEFINITIONS

Code of Practice for Information Security Management (ISO/IEC 27002:2005) - The international standard that defines guidelines and general principles for the effective management of information security within an organization. It is a risk-based framework widely used to guide establishment of security standards and management practices.

EDUCAUSE Association - A nonprofit association dedicated to the advancement of higher education through the effective use of information technology. Members include representatives from institutions of higher education, higher education technology companies, and other related organizations.

Family Educational Rights and Privacy Act (FERPA) – A Federal law enacted to protect access to student records and provide control over the disclosure of information from these records.

Gramm-Leach-Bliley Act (GLBA) - A Federal law enacted to control how financial institutions deal with the private information of individuals.

Health Insurance Portability and Accountability Act (HIPPA) – A Federal law enacted to set national standards for the security of electronic-protected health information.
Information Security - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

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 information technology security program.

Information Technology Security Program - A large combination of administrative, physical and technical protections, representing multiple layers of preventive, detective and corrective security controls strategically deployed to ensure the availability, integrity and confidentiality of the University's information resources.

International Electrotechnical Commission (IEC) - A global organization that develops and publishes standards addressing electrical, electronic, and related technologies. Membership comes from government, the private sector, consumer groups, professional associations, and others.

International Organization for Standardization (ISO) - The world’s largest developer of standards. The organization is made up of representatives from governmental and private sector standard bodies, e.g. the American National Standards Institute.

Payment Card Industry Customer Information Security Program (PCI) - A comprehensive set of payment application security requirements designed to ensure the confidentiality and integrity of customer information.

Virginia Alliance for Secure Computing and Networking (VA SCAN) - An organization formed to help strengthen information technology security programs within Virginia. The Alliance was organized and is operated by security practitioners and researchers from several Virginia higher education institutions.

D. SCOPE

This policy applies to all decision makers, developers and planners of campus systems and operations related to the conceptualization, design, acquisition, and maintenance of information technology.

E. POLICY STATEMENT

The University’s information technology security program is based upon best practices recommended in the Code of Practice for Information Security Management published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27002:2005), appropriately tailored to the specific circumstances of the University.

The program also incorporates security requirements of applicable regulations including, but not limited to, the Family Educational Rights and Privacy Act, Payment Card Industry Customer Information Security Program, Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act. Professional organizations, such as the national EDUCAUSE Association and the Virginia Alliance for Secure Computing and Networking, serve as resources for additional effective security practices.
The ISO/IEC 27002:2005 Code of Practice and other sources noted above are used to guide
development and ongoing enhancement of additional information technology security policies
as needed.

F. PROCEDURES

For security purposes, some procedures related to security are maintained internally.
Procedures are available on the Information Technology Services IT Policies website while those
maintained internally are available upon request to relevant parties as authorized by the
Information Technology Services.

G. RESPONSIBLE OFFICER

CIO and Associate Vice President for University Services

H. RELATED INFORMATION

University Policy 4100 – Student Record Policy
ITS Standard 01.2.0 - Assignment of IT Roles and Responsibilities
ITS Standard 02.1.0 - Internet Privacy
ITS Standard 02.2.0 - Workplace Device Technologies
ITS Standard 02.3.0 - Data Classification
ITS Standard 02.4.0 - IT Asset Control
ITS Standard 02.5.0 - Encryption
ITS Standard 02.6.0 - Virtual Private Network
ITS Standard 02.11.0 - Password Management
ITS Standard 04.1.0 - MIDAS Management
ITS Standard 04.2.0 - Account Management
ITS Standard 05.1.0 - IT Security Incident Handling
ITS Standard 05.2.0 - Data Breach Notification
ITS Standard 05.3.0 - Threat Detection
ITS Standard 05.4.0 –Virus & Malicious Code Protection
ITS Standard 06.1.0 - Facilities Security
ITS Standard 06.3.0 - Project Management
ITS Standard 06.4.0 - System Inventory
ITS Standard 06.5.0 - Server Management
ITS Standard 06.6.0 - Security Monitoring and Logging
ITS Standard 06.8.0 - IT Infrastructure, Architecture, and Ongoing Operations
ITS Standard 06.9.0 - Data Center Operations
ITS Standard 06.11.0 – System Change Management
ITS Standard 06.12.0 - Network Management
ITS Standard 06.13.0 - Desktop Management
ITS Standard 07.1.2 - Business Impact Analysis
ITS Standard 07.2.0 - Business Continuity and Disaster Recovery Plan
ITS Standard 08.1.0 - Risk Assessment
ITS Standard 08.2.0 – IT Security Program Review
ITS Standard 09.2.0 - Acceptable Use
ITS Standard 09.3.0 - Audit
POLICY HISTORY
************************************************************************
Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Rusty Waterfield             February 7, 2011
Responsible Officer Signature    Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks              December 14, 2010
Policy Review Committee (PRC),     Date
Chair Signature

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Robert L. Fenning            April 19, 2011
Responsible Oversight Executive Signature    Date

University Counsel Approval to Proceed:

/s/ Patrick B. Kelly             April 22, 2011
University Counsel             Date

Presidential Approval:

/s/ John R. Broderick            April 26, 2011
President                         Date

Policy Revision Dates:          October 1, 2007; April 9, 2010; April 26, 2011

Scheduled Review Date:          April 25, 2016