OLD DOMINION UNIVERSITY
University Policy

Policy #3505
INFORMATION TECHNOLOGY SECURITY POLICY

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: April 26, 2011

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

Most security procedures are maintained internally and may be available to relevant parties upon request to the Information Security Officer in the Office of Computing and Communications Services.

OCCS Procedure 1.2.0 - OCCS Data Center - Disposal of Data
OCCS Procedure 1.3.0 - OCCS Data Center - Off Campus Equipment Removal
OCCS Procedure 1.4.0 - OCCS Physical Security
OCCS Procedure 3.3.2.2 - Disaster Recovery Test Performance
OCCS Procedure 3.4.2.1 - Backup Tape Exchange
OCCS Procedure 3.4.2.2 - System Backups and Restoration Non Db
OCCS Procedure 3.4.2.3 - Review of Backup Logs
OCCS Procedure 3.4.2.6 - Protection of Backup Media Sent Off-Site
OCCS Procedure 4.1.1 - Project Management
OCCS Procedure 5.2.2 - Account Management
OCCS Procedure 5.4.4 - ODU Campus VPN Access
OCCS Procedure 6.3.2.1 - Encryption Key Management
OCCS Procedure 7.2.1 - Physical Access Control - Unauthorized Personnel
OCCS Procedure 7.2.2 - Safeguards for Protection Against Environmental Risk
OCCS Procedure 7.2.3 - Safeguard IT Systems and Data Not Residing in Primary Facility
OCCS Procedure 7.2.4 - Monitoring and Auditing Physical Access
OCCS Procedure 7.2.5 - Effective Environmental Controls
OCCS Procedure 7.2.6 - Controlled Access to Hardware and Facilities
OCCS Procedure 9.3.2.2A - Network Monitoring and Problem Escalation
OCCS Procedure 9.3.2.2B - nGenius Network Monitoring Start-up and Monitoring
OCCS Procedure 9.4.2 - Vulnerability Scanning

G. RESPONSIBLE OFFICER

Assistant Vice President for Computing and Communications Services

H. RELATED INFORMATION

University Policy 4100 – Student Record Policy
OCCS Standard 01.3.0 - Workplace Device Technologies
OCCS Standard 02.2.1 - Assignment of IT Security Roles
OCCS Standard 02.2.2 - IT Security Roles
OCCS Standard 02.3.2 - Business Impact Analysis
OCCS Standard 02.4.1 - Data Classification
OCCS Standard 02.4.5 - Internet Privacy
OCCS Standard 02.5.2 - System Inventory
OCCS Standard 02.6.2 - Risk Assessment
OCCS Standard 02.7.2 - IT Security Audit
OCCS Standard 02.8.0 - Security Program Review
OCCS Standard 03.2.2 - Continuity of Operations Planning
OCCS Standard 03.3.2 - Disaster Recovery - Business Continuity Plan
OCCS Standard 03.4.2 - IT System and Data Backup and Restoration

OCCS Standard 04.2.1 - Virus Protection
OCCS Standard 04.3.1 - Desktop Management
OCCS Standard 04.3.2 - IT System Security Plan
OCCS Standard 04.3.3 - Server Management
OCCS Standard 04.3.4 - Network Management
OCCS Standard 04.4.1 - Wireless Network
OCCS Standard 04.5.2 - Malicious Code Protection
OCCS Standard 04.6.2 - Project Management
OCCS Standard 05.2.2 - Account Management
OCCS Standard 05.3.2 - Password Management
OCCS Standard 05.3.3 - MIDAS 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 04.7.1 - IT Infrastructure, Architecture, and Ongoing Operations
OCCS Standard 06.2.1 - Digital Media
OCCS Standard 06.2.2 - Data Storage Media Protection
OCCS Standard 06.3.2 - Encryption
OCCS Standard 06.3.3 - E-Commerce
OCCS Standard 07.2.1 - Facilities Security
OCCS Standard 07.2.2 - Data Center Operations
OCCS Standard 07.2.3 - University Wiring
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
OCCS Standard 09.2.2 - Threat Detection
OCCS Standard 09.3.2 - Security Monitoring and Logging
OCCS Standard 09.4.2 - IT Security Incident Handling
OCCS Standard 09.5.2 - Data Breach Notification
OCCS Standard 10.2.1 - IT Asset Control
OCCS Standard 10.2.2 - Software License
OCCS Standard 10.2.3 - Service Level Agreements
OCCS Standard 10.4.1 - Change Management
OCCS Guideline 1.0.0 - Cloud Computing Guidelines for Faculty and Staff
OCCS Guideline 1.0.1 - Best Practices in Protecting University Data
OCCS Guideline 4.3.4.1 - Firewall Best Practices
OCCS Guideline 4.3.4.2 - Router-Switch Best Practices
OCCS Guideline 8.3.2 - IT Security Awareness and Training Program

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), Chair Signature — Date

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