OLD DOMINION UNIVERSITY
University Policy

Policy #3502
INFORMATION TECHNOLOGY INFRASTRUCTURE, ARCHITECTURE, AND ONGOING OPERATIONS 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 University's commitment to establishing specific standards, guidelines and procedures affecting key components of its information technology (IT) infrastructure, architecture, and ongoing operations.

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

N/A

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 will establish specific standards, guidelines, and procedures that influence decisions affecting key components of its IT infrastructure, architecture, and operations. These standards, guidelines, and procedures will be reviewed periodically to assure they conform to best practices as described by the ISO/IEC 17799, Information Technology - Code of practice for information security management, EDUCAUSE, Internet2, and others within higher education, as well as those from selected technology industries.

Research or other institutional endeavors by their nature may require the use of technology and practices not yet appropriate for normal use. The ultimate goal of this policy is to create logical relationships between information technology resources and the mission of the University and its units.

F. PROCEDURES

For security purposes, some procedures related to infrastructure, architecture and ongoing operations are maintained internally. Procedures are available on the OCCS website and are linked below, while those maintained internally are available upon request to relevant parties as authorized by 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 - Removal of Equipment for Offsite and Personal Use
OCCS Procedure 1.4.0 Procedures for Access and Physical Security of OCCS Data Center
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 7.2.1 - Physical Access Control - Unauthorized Personnel
OCCS Procedure 7.2.2 - Safeguards for Protection Against Human, Natural and 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 Network Facilities
OCCS Procedure 9.3.2.2A - Monitoring and Problem Escalation
OCCS Procedure 9.3.2.2B - nGenius Monitoring and Startup
OCCS Procedure 9.4.2 - Vulnerability Scanning

G. RESPONSIBLE OFFICER

Assistant Vice President for Computing and Communications Services

H. RELATED INFORMATION

OCCS Standard 04.7.1 - IT Infrastructure, Architecture, and Ongoing Operations

For more information regarding the management of technology infrastructure, please refer to the following sources:

The Campus Cyberinfrastructure Working Group of Net@EDU helps educational institutions develop institutional strategies and plan their resource deployment in this emerging and evolving technological landscape and helps their users harness and optimize the power and capabilities of new integrated IT tools and systems for educational and research applications in higher education.

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

Internet2 develops and deploys advanced network applications and technologies for research and higher education, accelerating the creation of tomorrow's Internet.

ISO/IEC 17799/27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC).

The National LambdaRail develops and deploys a fiber optic network infrastructure for the purpose of advancing research, clinical, and educational goals.

The Postsecondary Electronic Standards Council is a non-profit association of colleges and universities; professional and commercial organizations; data, software and service providers; and state and federal government agencies.

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 — October 26, 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