



OLD DOMINION UNIVERSITY

University Policy

Policy #3509

SOFTWARE DECISION ANALYSIS POLICY

Responsible Oversight Executive: Vice President for Administration and Finance

Date of Current Revision or Creation: May 4, 2012

A. PURPOSE

The purpose of this policy is to ensure that software-based technologies, applications and services meet University information technology requirements, are compatible with existing technology standards and services, and are aligned with information technology priorities.

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

Project Management Office (PMO) - A strategic functional unit within the Office of Computing and Communications Services that promotes and advances project management principles and services for Information Technology (IT) projects at Old Dominion University.

Software Technologies, Applications and Services - Computer programs or a group of computer programs and related data that operate on or interact with the University systems and information technology resources. These include, but are not limited to, system software, application software, programming software, software as a service delivery model, servers and utilities.

D. SCOPE

This policy applies to all employees and employees of affiliated organizations in academic and administrative units who procure software technologies. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. 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.

E. POLICY STATEMENT

Software technologies, applications and services are to be implemented in ways that promote the security of systems and data and contribute to the effectiveness and efficiency of the institution. Prior to procurement, the Office of Computing and Communications Services (OCCS) will conduct an evaluation and assess security, policy and regulatory compliance issues; operational and support issues; and integration with existing University services, systems and standards.

This policy applies to all software technologies, applications and services that meet one or more of the following criteria for review, regardless of who initiates the acquisition or the origin of the funding source:

- requires the use of University IT systems and resources;
- requires on-going maintenance by OCCS;
- collects, stores, displays, or exports personally identifying data, non-public personal financial information, protected health information, or student records or will store or manage data that is subject to legal controls (Ex. FERPA, HIPAA);
- interfaces with an existing enterprise system application, such as MIDAS, Banner, course management system, etc.;
- has implications for physical safety.

This policy will apply to single quantity, open-source, commercially available or independently developed software only if it meets one or more of the criteria above. Anyone who is uncertain about whether a planned acquisition or development of software technology, application or service is subject to this policy should contact OCCS.

Departments and administrative units contribute to and share responsibility for the deployment of software technologies, applications and services. Specifically, they are responsible for:

- gathering information on software technologies, applications and services;
- initiating a software review with the PMO prior to the procurement;
- completing [the IT Security and Integration Review](#) document to assist the review process.

The PMO is responsible for accepting and tracking requests for reviews and coordinating timely responses to the departmental or administrative units.

OCCS is responsible for reviewing submissions and making recommendations to departments and administrative units. The review will include at a minimum:

- an analysis of compliance with regulatory and University policy;
- technical review;
- security review;
- operational review;
- ongoing maintenance and cost of ownership review.

OCCS will use the following standards and guidelines for reviewing and making recommendations:

- compatibility with the University's network environment;
- compliance with the University's security policy;
- suitability based on needs assessment;
- licensing compliance for software purchase;
- hardware and software that can be efficiently supported;
- availability of sufficient University resources (including initial and recurring costs).

The outcome of the review will be an analysis of the technology's ability to be compliant with and successful in the University's IT environment. If applicable, recommendations will be made to prevent or mitigate risks. Software acquisitions that are not aligned with OCCS' recommendations will not be supported without approval of the agency head.

F. PROCEDURES

1. Departments determine whether the policy applies for the Information Technology software, system or service planned for implementation at Old Dominion University. The policy only applies for Information Technology software, system, or services that meet (with an answer of yes) one or more of the criteria below.
 - a. Does the system, software, or service require installation on University servers or the implementation of new server resources?
 - b. Does the system, software, or service require OCCS to implement changes to the University network (to include wireless network)?
 - c. Does the system, software, or service require on-going maintenance by OCCS?
 - d. Does the system, software, or service collect, store, display, or export personally identifying data, non-public personal financial information, protected health information, or student records or will store or manage data that is subject to legal controls (Ex. FERPA, HIPAA)?
 - e. Does the system, software, or service interface with an existing enterprise system application, such as MIDAS, Banner, course management system, etc.?
 - f. Does the system, software, or service have implications for physical safety?
2. Departments or administrative units gather specific information about the software from the vendor according to the [IT Security and Integration Review](#) document provided by OCCS to assist in the data collection. The information will consist of technical material, hardware requirements, vendor practices, security, consulting, etc. OCCS staff will be available to consult upon request. Early planning is strongly encouraged in order to avoid unnecessary delays.
3. OCCS assesses the information with technical support staff and/or the vendor for further clarification as needed on specific items on the Review document. In most cases, the depth of the review is minimal and can be performed in a timely manner, i.e., within 30 calendar days.
4. Following the assessment, OCCS provides recommendations, a preliminary project timeline and key performance indicators.

Questions regarding this procedure should be directed to the Project Management Office in OCCS at 757.683.3189 or by email at pmo@odu.edu.

G. RESPONSIBLE OFFICER

Assistant Vice President for Computing and Communications Services

H. RELATED INFORMATION

The deployment of information technology applications must adhere to all applicable University Policies as noted below. For the Standards associated with University Policies, see also <http://occs.odu.edu/policies/index.php>

[University Policy 3500 - Policy on the Use of Computing Resources](#)

[University Policy 3502 - Information Technology Infrastructure, Architecture, and Ongoing Operations Policy](#)

[University Policy 3505 - Information Security Policy](#)

[University Policy 3508 - Information Technology Project Management](#)

[Department of Procurement Services Procurement Manual](#)

