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.

This policy and supporting procedures and guidelines are not intended to produce service interruptions or introduce other risks into the efficient operation of business at the University.

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning 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.


Code of Virginia Section 23.1-1002, as amended, Eligibility for Restructured Financial and Administrative Operational Authority and Financial Benefits

C. DEFINITIONS

Project Management Office (PMO) - A strategic functional unit within the Office of Information Technology Computing and Communications Services (ITS) 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 who are paid through the University 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 through an operating agreement and include the Foundations, the Community Development Corporation, and the Alumni Association.

This policy applies to all software technologies, applications and services, including single quantity, open-source, commercially available or independently developed software, that are determined to 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, with exceptions as noted in ITS Guidelines;
- requires on-going maintenance by ITS;
- collects, stores, displays, or exports personally identifying data, non-public personal or financial information, protected health information, or students 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.; or
- has implications for physical safety.

NOTE: Anyone who is uncertain about whether a planned acquisition or development of software technology, application or service is subject to this policy should contact ITS.

The software decision analysis process, in collaboration between the requesting department, Procurement and ITS, is one way to apply due care in expanding adoption of information security reviews. In cases where systems are purchased prior to completing a software security review or system risk assessment, other controls are in place that serve to lower risks until such a review is completed. It remains the responsibility of the requesting department to initiate and complete the appropriate review.

E. POLICY STATEMENT

Software technologies, applications and services are to be implemented in ways that contribute to the effectiveness and efficiency of the institution, and that promote compliance with University standards, the security of systems and data and contribute to the effectiveness and efficiency of the institution. Prior to procurement of any new software technologies, applications or services, the System Owner will initiate with the Office of Computing and Communications Information Technology Services (ITSOCCS) an evaluation to assess integration requirements with existing University services, systems and standards, and operational support requirements. will conduct an evaluation and assess security, policy and regulatory compliance issues; operational and support issues; and integration with existing University services, systems and The primary goals are determination of integration challenges or coordination needs, information gathering for initiating an IT project, assistance in assessment of redundant services that may be leveraged, assistance with maintenance and cost analysis when appropriate, fostering appropriate dialogue
among various stakeholders and operating units, and resource planning. Additional benefits include documentation of the specific data that is involved, gaining Data Owner approval for use of the data, facilitating the proper contract addendum for sharing the data, and supporting Identity and Access considerations according to ODU IT security 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 decision analysis review with the ITS PMO prior to the procurement;
- completing the IT Security and Integration Review document to assist the review process;
- understanding information security roles and responsibilities;
- supporting University standards and compliance; and
- ongoing maintenance and cost of ownership.

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

ITSOCCS is responsible for reviewing submissions and sharing findings with making recommendations to departments and appropriate administrative units. The review will include at a minimum:

- an analysis of compliance with Federal and State regulations and University policy;
- a technical review, including a security review and an integration review when appropriate; and
- security review;
- operational review;
- ongoing maintenance and cost of ownership review, when appropriate.
ITSOCCS and the requesting department will use the following standards and guidelines for reviewing and making recommendations:

- compatibility with the University’s computing and network environments;
- compliance with the University’s IT standards/security policy;
- suitability based on needs assessment;
- licensing compliance for software purchase;
- hardware and software that can be efficiently supported; and
- 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 ITSOCCS’ recommendations will not be supported without approval of the requesting department’s Vice President/agency head.

F. PROCEDURES

The requesting department applies this policy for the Information Technology software, system or service planned for implementation at Old Dominion University according to the criteria establishing within this policy.

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?

2.1. The requesting departments or administrative units gathers specific information about the software from the vendor according to the IT Security and Integration Review document provided by OCCS and submits an ITS Software Decision Analysis Request to ITS to assist in the data collection. Other information needed will consist of technical documentation/material, hardware requirements, vendor practices, security, consulting, etc. ITSOCCS staff will be available to consult upon request. Early planning is strongly encouraged in order to avoid unnecessary delays.

3.2. ITSOCCS 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 time required to complete a review can vary based on the complexity/depth of the system review.
is minimal and the timing can be performed in the academic and budget cycles of the University in a timely manner, i.e., within 30 calendar days.

4.3. Following the assessment, ITS OCCS provides recommendations, a summary of findings, including whether contract protections are needed via use of an Addendum Form, whether further architectural review is needed, whether an IT project is needed, and data ownership and responsibilities; preliminary project timeline and key performance indicators.

5.4. The departmental System Owner for the requested system will sign-off on the ITS findings, acknowledging security responsibilities as the System Owner, and when ODU data is involved, the Data Owner(s) will sign off for approval for the use of the data.

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

G. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the Commonwealth’s Records Retention Schedules.

H. RESPONSIBLE OFFICER

CIO and Associate Vice President for University Services

I. 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://www.odu.edu/about/policiesandprocedures/computing

University Policy 3500 - Policy on the Use of Computing Resources
University Policy 3502 - Information Technology Infrastructure, Architecture, and Ongoing Operations Policy
University Policy 3504 – Data Administration Policy
University Policy 3505 - Information Security Policy
University Policy 3508 - Information Technology Project Management
Department of Procurement Services Procurement Manual