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, without introducing unnecessary service interruptions or other risks to 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.


C. DEFINITIONS

Data Owners - University employees (typically at the level of Registrar or Unit Director) who oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area. They are responsible for decisions about the usage of institutional data under their purview.

Project Management Office (PMO) - A strategic functional unit within the Office of Information Technology 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.

System Owner – Manager or departmental head responsible for operation and maintenance of a University IT system or oversight of hosted systems under their purview.
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 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.; or
- has implications for physical safety.

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 promote compliance with University standards. Prior to procurement of any new software technologies, applications or services as defined within the scope of this policy, the System Owner will initiate with Information Technology Services (ITS) an evaluation to assess integration requirements with existing University services, systems and standards, and operational support requirements. 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 are 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.

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 with the ITS PMO prior to the procurement;
- understanding information security roles and responsibilities;
• supporting University standards and compliance;
• conducting ongoing maintenance; and
• managing 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.

ITS is responsible for reviewing submissions and sharing findings with departments and appropriate administrative units. The review will include:

- 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
- ongoing maintenance and cost of ownership review, when appropriate.

ITS 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 and Software Decision Analysis and System Risk Analysis Guideline;
- 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 do not meet ITS recommendations will not be supported without approval of the requesting department’s Vice President.

F. PROCEDURES

1. Departments considering a planned acquisition or development of software technology, application or service is subject to this policy and should contact ITS.

2. The requesting department gathers information about the software and submits an ITS Software Decision Analysis Request to ITS to assist in the data collection. Other information needed will consist of technical documentation, hardware requirements, vendor practices, security, consulting, etc. ITS staff will be available to consult upon request. Early planning is strongly encouraged in order to avoid unnecessary delays.

3. ITS assesses the information with technical support staff and/or the vendor for further clarification as needed on specific items on the review document. The time required to complete a review can vary based on the complexity of the system and the timing in the academic and budget cycles of the University.

4. Following the assessment, ITS provides 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.
5. 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.

The software decision analysis process, in collaboration among the request 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 review is completed. It remains the responsibility of the requesting department to initiate and complete the appropriate review, as required by this policy.

Questions regarding this policy should be directed to the Project Management Office in ITS 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

Associate Vice President and CIO, Information Technology 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
Information Technology Services Standard 08.1.0 – Risk Assessment Standard
Department of Procurement Services Procurement Manual
POLICY HISTORY
************************************************************************
Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Rusty Waterfield _____________________________ July 25, 2019 _____________________________
Responsible Officer _____________________________ Date _____________________________

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks _____________________________ January 22, 2018 _____________________________
Chair, Policy Review Committee (PRC) _____________________________ Date _____________________________

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Gregory DuBois _____________________________ July 25, 2019 _____________________________
Responsible Oversight Executive _____________________________ Date _____________________________

University Counsel Approval to Proceed:

/s/ R. Earl Nance _____________________________ July 31, 2019 _____________________________
University Counsel _____________________________ Date _____________________________

Presidential Approval:

/s/ John R. Broderick _____________________________ August 1, 2019 _____________________________
President _____________________________ Date _____________________________

Policy Revision Dates: May 4, 2012; August 1, 2019

Scheduled Review Date: July 31, 2024