OLD DOMINION UNIVERSITY
University Policy

Policy #3509
SOLUTIONS DISCOVERY ANALYSIS (SDA) POLICY

Responsible Oversight Executive:	Vice President for Digital Transformation and Technology
Date of Current Revision or Creation:	July 10, 2024

A. PURPOSE

The purpose of this policy is to ensure that software-based technologies, applications, and services are thoroughly reviewed to meet information technology security regulations and associated business requirements and are compatible with existing technology standards and services 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 7.01(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 Sections 23.1-1000-1028, as amended, Restructured Higher Education Financial and Administrative Operations Act

C. DEFINITIONS

Data Compliance Owners – As defined in Information Technology Services Standard 01.2.0 - IT Security Roles & Responsibilities, University employees (typically at the level of Unit Leader) 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. Data compliance owners understand the compliance requirements for their data, designate the compliance level of their data and approve access to their data. University Data Compliance Owners oversee compliance for data that is shared or leveraged across the University, such as Human Resources, Finance, Financial Aid, and Student FERPA data. Departmental Data Compliance Owners oversee the data that is specific to the departmental application or system that is not overseen by one or more of the University Data Compliance Owners.

Information Security Governance, Risk, and Compliance (GRC) – A strategic functional unit within the University Information Security Office serving the campus community by assisting with meeting compliance of federal and state regulations; University policies, standards, and guidelines; and managing potential security risks to the University. The GRC team also seeks to

provide University leadership with the tools needed to make informed risk-based decisions that best support the mission of the University.

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.

Services – Professional services to include consulting, designing, organizing, and managing University environments to include access to University data, to assist or do work on behalf of University employees. Consultation to departments on security aspects related to potential software purchases, ensuring alignment with our overall security objectives.

Software Technologies and Applications - Computer programs or a group of computer programs and related data that process, store, or access University data, 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, whether delivered as software as a service (cloud-based), hosted, or on-premises installed on ODU systems.

System Compliance Owner – As defined in Information Technology Services Standard 01.2.0 - IT Security Roles & Responsibilities, a manager or departmental head responsible for operation and maintenance of a University IT system or overseeing hosted systems under their purview. System Compliance Owners are responsible for the overall compliance and security of their system.

D. SCOPE

This policy applies to all employees who procure software technologies or solutions that integrate or access University systems or University data. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University.

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) to include data classifications 1 through 4 per Information Technology Services Standard 02.3.0 Data Administration & Classification;
- 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 Information Security GRC.

The Solutions Discovery Analysis process, in collaboration among 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 solutions security review or system risk assessment, it will remain the responsibility of the requesting department to initiate and complete the review in collaboration with Information Security GRC.

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 comply with University, state and federal standards. Prior to procurement of any new software technologies, applications, or services as defined within the scope of this policy, the System Compliance 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 Compliance Owner approval for the use of the data or access, 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:

- initiating a Solutions Discovery Analysis (SDA) prior to the procurement;
- following University policies, and other standards as applicable; and
- identifying and managing ongoing total cost of ownership.

The ITS Project Management Office is responsible for (i) accepting and tracking requests for reviews, (ii) coordinating timely responses to the departmental or administrative units, and (iii) requesting information on software technologies, applications, and services.

Information Security GRC 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 apply the following standards and guidelines for reviewing and making recommendations:

- discovery of business need, workflows, and processes;
- review of solution options within existing IT environment;
- review of external solution options;
- compatibility with the University's computing and network environments;
- compliance with the University's IT standards and Solutions Discovery Analysis and System Risk Analysis Guideline;
- suitability based on available solutions;
- licensing compliance for software purchase;
- hardware and software that can be reasonably supported;

- availability of sufficient University resources (including initial and recurring costs); and
- ensuring data access is approved by appropriate Data Compliance Owners.

The outcome of the review will be an analysis of the technology or service's ability to be compliant with and successful in the University's IT environment. If applicable, recommendations will be made to prevent, mitigate, or accept risks. Solution acquisitions that are not aligned with ITS recommendations will not be supported without approval of the requesting department's Vice President or equivalent for Class 1 data or appropriate stakeholder for Class 2-4 data.

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 established within this policy.

1. Departments considering a planned acquisition or development of software technology, application, or service are subject to this policy and should contact the IT Project Management Office which will initiate the Solutions Discovery Analysis process.

2. The requesting department gathers information about the solution and submits an ITS Solutions Discovery 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. Information Security GRC assesses the information with technical support staff and/or the vendor for further clarification as needed on specific items in 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 including whether contract protections are needed via use of the relevant Addendum Form, whether further architectural review is needed, whether an IT project is needed, and identification of data compliance ownership and responsibilities.

5. The departmental System Compliance Owner for the requested system will sign-off on the ITS findings, acknowledging security responsibilities as the System Compliance Owner, and when ODU data is involved, the Data Compliance Owner(s) will sign off for approval for the use of the data as well as other designated roles such as system administrator or application administrator when warranted.

Questions regarding this policy should be directed to the Information Security GRC Office via email at itsriskandcompliance@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:

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 Technology Security Policy
University Policy 3508 - Information Technology Project Management
Information Technology Services Computing Policies and Standards
Information Technology Services Standard 02.3.0 – Data Administration & Classification Standard
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/ Kirk Dewyea — July 2, 2024
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna Meeks — May 28, 2024
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Nina R. Gonser — July 2, 2024
Responsible Oversight Executive — Date

University Counsel Approval to Proceed:

/s/ Allen T. Wilson — July 10, 2024
University Counsel — Date

Presidential Approval:

/s/ Brian O. Hemphill — July 10, 2024
President — Date

Policy Revision Dates: May 4, 2012; August 1, 2019; July 10, 2024

Scheduled Review Date: July 10, 2029