Standard for the Procurement of Information Technology Applications

1. Purpose

Information technology applications are essential to the university's ability to achieve its missions and goals. These computing solutions must be implemented in ways that promote security of systems, data, and persons; and that contribute to the effectiveness and efficiency of carrying out university functions. Departmental or distributed university units as well as the *Information Technology organization* contribute to and share responsibility for the deployment of these computing solutions.

This standard seeks to ensure that, prior to procurement, these *information technology applications* have a high probability of achieving the following objectives:

- A secure implementation that protects university resources, including infrastructure and information
- Use of university resources that is made effective through adherence to technology standards for integration, support, and information technology architecture

Terms in italics are defined in section 4.

Information Technology Acquisitions (ITA) is the university office charged by University Policy 3015, "University Contract Signature Policy and Procedures," to be the point of contact for all contracts related to computer hardware and software. (*www.policies.vt.edu/3015.pdf*). "Contract signature authority is delegated by the Director of Materials Management to the Director of ITA." The policy further states that ITA "reviews, obtains legal counsel's review, and signs all contracts for computer hardware, software, including those contracts involving money, not for money, for testing, and maintenance agreements." Policy 3015 documents the contractual and spending limits for departments.

2. Requirements

For any acquisition of information technology applications that is

- a procurement against an existing university contract of an information technology application that exceeds departmental purchasing authority; and/or
- a procurement requiring a new contract for information technology applications,

departments must document to ITA that the required reviews have been satisfactorily completed.

Departments procuring information technology applications from existing university contracts and within their signature authority are encouraged to assure that these procurements meet the requirements as well.

The purpose of the reviews below is to minimize expenditures of effort and funds on software applications that may not be useable due to issues with university liability—particularly regarding system security and personal information, and/or implications for the provision of resources beyond the procurement itself.

Does the purchase require a security review?

Security reviews are required if:

- the information technology application qualifies as an *enterprise-level software application*;
- the application collects, stores, displays, or exports *personally identifying covered data, non-public personal financial information, protected health information,* or *student records*;
- the information technology application has implications for physical safety.
- the application requires an interface with an existing enterprise system, such as an enterprise authentication service, Banner, Scholar, the enterprise data warehouse.

Does the purchase require review by one or more data stewards?

Data steward reviews are required if:

- the application collects, stores, displays, or exports *personally identifying covered data, non-public personal financial information, protected health information,* or *student records*.

Does the purchase require a review of enterprise architecture?

Architectural reviews are required if:

- the information technology application qualifies as an *enterprise-level software application*;
- the application requires an interface with an existing enterprise system, such as an enterprise authentication service, Banner, Scholar, the enterprise data warehouse.

Does the purchase require a review of network architecture?

Network reviews are required if the application requires non-standard configurations of the university network.

Does the purchase require a review of Information Technology-provided support or services?

Reviews are required if the requested support or service is new.

Is the deployment of the procured application a candidate to be classified as a *major project* under the university's *restructuring management agreement* (*www.vt.edu/restructuring/*)?

Information Technology can assist in the determination of whether an acquisition and its deployment constitute a major project.

3. Procedures

Information Technology Acquisitions provides procedures, information, and contacts for departments to assure that the required reviews have been completed, and can provide additional information as may be

required. ITA is also available to answer questions and direct departments to resources for procurements of information technology applications that are within the departmental authority.

4. Definitions

Data stewardship refers to oversight of the capture, maintenance and dissemination of data for a particular operation. Data stewards have key responsibilities for data management activities.

Enterprise-level software applications, or, briefly, "enterprise systems," provide business logic for enterprise-level functions such as authentication services, financial transactions, student systems, e-mail, human resources, purchasing, content management, and many other functions critical to the ongoing functioning of the university. Enterprise-level applications must be secure, scalable, and reliable for continuous operation. Enterprise-level applications are typically multi-user and long-lived. Enterprise-level applications may serve major segments of the university community (for example, available to all students or to all employees), or provide a particular function to the entire community (for example, parking permits). Enterprise-level applications are not limited to those provided by or hosted by the Information Technology organization.

Enterprise-level software applications are defined here as distinct from:

> **Department-level software applications**, for the purposes of this policy, provide similar business logic for functions below the breadth of enterprise systems. In the university context, these may be run by specific departments, colleges, centers, senior management areas, or any other university unit.
>
> **Individual-level software applications** address the needs of individuals to create and manage information, typically through an individual-use device (including desktop workstations, portable computing devices, or Internet-access devices). Examples include word processing, spreadsheets, e-mail client software, media editing. Individual-level software applications exist in contrast to enterprise-level software applications and department-level software applications.

Information Technology Acquisitions is the unit charged with acquiring technology goods and services for the university using best value concepts.

Information technology application, for the purposes of this policy, refers to software applications that are either *enterprise-level software applications* or d*epartment-level software applications*.

The **Information Technology** organization refers to the units within the university within the administrative oversight of the Vice President for Information Technology and Chief Information Officer.

Major projects are defined by the restructuring management agreement. Deployments that are very high cost or broad scope are candidates for such a classification. The Vice President for Information Technology can assist in determining major project status under current definitions. Projects that are determined to be "major" have additional state reporting requirements.

Nonpublic personal financial information includes any paper or electronic record containing nonpublic personal financial information provided by students or others in order to obtain a financial product or service from the university, including loan applications, bank and credit card numbers, account histories, Social Security numbers, income tax returns, credit reports and other related customer information. (See Policy 7025, Safeguarding Nonpublic Customer Information, that provides university implementation of the Gramm-Leach-Bliley Act or GLBA.)

Procurements that are covered by this policy may come from a number of methods of acquisition, including purchases, contracts for services, gifts, or third-party services provided at no cost to the university.

The **restructuring management agreement** delineates Virginia Tech's authority for certain operations under the Restructured Higher Education Financial and Administrative Operations Act of 2006. (See *www.vt.edu/restructuring/*.)

Personally identifying covered data includes Social Security numbers, credit card numbers, debit card numbers, bank account numbers, driver's license numbers, passport numbers, and name in combination with full date of birth.

Protected health information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual, as defined in the Health Insurance Portability and Accountability Act (HIPAA).

Student records include all student data that is covered by the Family Educational Rights and Privacy Act (FERPA) which includes records, files, documents, and other materials that contain information directly related to a student; and are maintained by the university, excepting law enforcement records, "sole possession" records, and non-student employee records. (See United States Code—20 U.S.C. § 1232g, and the "Confidentiality of Student Records" at *www.registrar.vt.edu/records/ferpa.php*.

5. References

The deployment of information technology applications must also adhere to all other applicable university policies. Policies of particular importance for deploying information technology applications include those listed below, along with standards associated with them. See also *www.it.vt.edu/administration/policies.html*.

- Policy 2010 Release of Names and Addresses of Students, Faculty, Staff, and Alumni
- Policy 3015 University Contract Signature Policy and Procedures
- Policy 5617 Safety and Security Camera Acceptable Use Policy
- Policy 7000 Acceptable Use of Computer and Communication Systems
- Policy 7010 Policy for Securing Technology Resources and Services
- Policy 7040 Personal Credentials for Enterprise Electronic Services
- Policy 7100 Administrative Data Management and Access Policy
- Policy 7105 Policy for Protecting University Information in Digital Form
- Information Technology Standard for Storing and Transmitting Personally Identifying Information (*www.it.vt.edu/publications/pdf/3_PIIStandardFinal13June-signed.pdf*)

- Information Technology Standard for Protecting Sensitive University Information Used in Digital Form (*http://www.it.vt.edu/publications/pdf/2_SensitiveDataStandardRevision1-signed.pdf*)
- Information Technology Security Standards for Social Security Numbers (*http://www.computing.vt.edu/administrative_systems/banner/security%20standards_5July05.pdf*)
- Policy 7200 University IT Security Program
- Policy 7210 Information Technology Project Management
- Information Technology Project Management Standard (*https://secure.hosting.vt.edu/www.itplanning.org.vt.edu/pm/)*
- Policy 7205 IT Infrastructure, Architecture and Ongoing Operations

Also see:

- Virginia Tech Board of Visitors, "Information Technology Security and Authority Resolution," June 4, 2007 (http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf).
- § 2.2-2006 of the Code of Virginia http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2006

6. Approval and Revisions

This standard supersedes Policy 10100, Policy for the Purchase of Departmental-Based Computer Systems.

Approval

Approved, Vice President for Information Technology and Chief Information Officer, Earving L. Blythe

(Signed) Earving L Blythe

Digitally signed by Earving L Blythe
DN: dc=edu, dc=vt, c=US, o=Virginia Polytechnic Institute and State University, cn=Earving L Blythe, 0.9.2342.19200300.100.1.1=809628, serialNumber=1231
Date: 2011.01.19 13:18:45 -05'00'

Date _____