The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

Information Technology Standard: IT Infrastructure, Architecture, & Ongoing Operations Standard
Reference Number: 09.2.0
Date of Current Revision or Creation: February 2013

A. PURPOSE

The purpose of this standard is to describe the applicable standards and guidelines for the information technology infrastructure, architecture, and ongoing operations.

B. DEFINITIONS

Middleware is computer software that connects other software or applications and allows for the exchange of data.

C. STANDARDS STATEMENT

Technology choices are made to best align with the strategic direction of the University, to meet the needs of existing and planned applications, to support prevailing and developing industry trends and to make the most efficient use of resources.

Networking and Telecommunications

Old Dominion University's networks follow the Internet standards as implemented by the higher education community. The key standards areas and the inter-institutional efforts that influence standards adoption are listed below.

- The set standards defined by the Internet Engineering Task Force (IETF) that form the technical foundation for Higher Education networks
- The Institute of Electrical and Electronics Engineers (IEEE) networking standards, in particular the IEEE 802.x series of standards
- The EIA/TIA standards for building telecommunications wiring and facilities
- The ATM Forum
- The Center for Internet Security (CIS) for router and switch configuration security benchmarks
- Implementation of the networking standards needed to connect to Internet2’s Abilene network.
- Implementation of the networking standards needed to connect to the National Lambda Rail network.

**Computing Hardware, Storage, and Operating Systems**

Decisions on which operating systems to support and what storage environments to build are primarily based on strategic direction, the needs of existing and planned applications, staff expertise, industry trends, and efficient use of resources in operating the environment as a system. Relevant standards are leveraged when making the best decisions.

**Computing Hardware**

Hardware selection for central computing is based on the specific needs of applications. Computationally intensive applications and computational science, in general, will often require the use of emerging technologies that may not yet be appropriate for general purpose computing.

- The de facto standard Intel platform that runs a variety of operating systems including Microsoft Windows, Unix, Linux and X86 based Solaris.
- Computing platforms that run Sun Solaris, IBM AIX, SGI IRIX, and other common UNIX derivatives.
- Hardware selection for desktop computing is driven by the needs of application users. Researchers often have different desktop computing needs than typical information workers. The CPU, memory, disk resources, display resources, and input devices are tailored to the needs of applications the user requires.
- Apple platforms that run Mac OS X

**Storage**

Storage selection is driven by application considerations such as selection and retrieval of data, retention requirements, anticipated growth, and expected response time.

- American National Standards Institute (ANSI) for Fiber Channel, SCSI, and various other storage connectivity standards.
- Network Attached Storage de facto standards such as the Sun Microsystems developed NFS and Secure-NFS protocols and Microsoft’s CIFS
- Backup and Recovery solutions are typically implemented using tools provided by the operating system or specialized solutions with decisions made as the result of a negotiated procurement

**Operating Systems**

ODU’s practice, where possible, is to use open source operating systems. Other considerations are vendor application certification or supported environments, performance, and security.

- De facto standards such as the Microsoft Windows and Apple Mac OS family of operating systems
- The common flavors of UNIX such as Sun Solaris, IBM AIX, Linux, etc., supporting IEEE POSIX complaint applications interface
- Other operating systems needed to host specific environments e.g. z/OS on IBM mainframes, etc.

**Middleware**

Middleware and the decisions regarding the middleware components selected for use on higher education networks are heavily influenced by national and international activities in this space. The critical sets of standards and influential higher education activities are listed below.

- The selection of technologies made by the National Science Foundation for the NSF Middleware Initiative. This includes Directory Schema, Web Initial Sign-On (Web-ISO), Public Key Infrastructure (PKI), Grid Technology, Shibboleth and SAML, and other associated standards and software systems.
- The Internet2 Middleware Initiative and the Middleware Architecture Committee for Education (MACE) has developed and coordinated a selection of middleware technologies specifically targeted towards the needs of and interoperability between institutions of higher education. These include standards for directory schema for the representation of people and groups, inter-institutional authentication and authorization systems, user management and provisioning, PKI, and other similar technologies.
- The proceedings from the Internet2/EDUCAUSE Campus Architecture Middleware Planning (CAMP) sessions.
- National and international standards such as those from the Internet Engineering Task Force (IETF), the Organization for the Advancement of Organized Information Standards (OASIS), the International Telecommunications Union (ITU), and other similar organizations that have standardized technologies such as X.500, X.509, LDAP, XML, SAML, SASL, S/MIME, and SSL/TLS.
- The RSA Data Security de facto standards for public key cryptography.

**Databases**

Decisions about database products are based upon the requirements of University applications. Existing database solutions (e.g. those already supported by the institution) are generally preferred over different but equivalent technology.

- The use of relational database technologies and SQL are considered best practices. Relational databases and the query language are well-understood and have a long history of successful application in a variety of applications.
- Object-relational mapping strategies are preferred over object-oriented databases, as the requirements for long-term success with the latter are not as well understood as relational databases.
- The use of database access standards that avoid database vendor lock-in is a best practice. For example, the Java Database Connectivity (JDBC) API allows Java applications to work with relational databases in a vendor-independent manner.

**Systems Management**

Systems management concerns the monitoring of system and network components for faults and performance, accounting for the use of resources, configuration management, and the intersection...
between security policy and the operating practices that lead to a secure IT infrastructure. The goal of systems management is management of the IT environment as a whole. Guidelines on systems management are largely derived from the ISO FCAFS framework, along with the supporting standards for network management as defined by the IETF.

Security

A comprehensive IT security program includes policy, user awareness, and training coupled with strong technical controls on computer and network systems, the associated data, and data transmission. Mechanisms for the proper protection of systems and their associated data are drawn from a variety of standards bodies and industry best practices including those listed below.

- The Internet Engineering Task Force (IETF)
- The SANS Institute
- The Center for Internet Security (CIS) benchmarks and tools
- The National Institute of Standards and Technology (NIST) and their Federal Information Processing Standards (FIPS)
- American National Standards Institute (ANSI)
- Virginia Alliance for Secure Computing and Networking (VA SCAN)
- EDUCAUSE
- The ISO 27000 family of standards – guidelines and general principles for security

Applications

In general, the application infrastructure and operations are managed with an emphasis on cost containment. They are also provisioned on the basis of perceived value or future needs. Given the diverse missions and needs of the University, the portfolio of applications can be divided into two distinct groups.

Enterprise applications support the mission-critical operations and include systems to manage student information, human resource and financial processes and support collaboration, portals, digital repositories, content management and web applications. Enterprise applications at the University also include systems unique to higher education such as learning management systems. Decisions regarding enterprise applications are centralized and there is an emphasis on deploying integrated technologies that are mature, stable, secure, and proven in the field.

Desktop applications support the individual needs of faculty, staff, and students at the University and are typically office productivity applications used by knowledge workers. Decisions about desktop applications are distributed across departments and business units. Desktop applications at the University include word processing, spreadsheet, presentation, database, Internet browser, communication and mail client software.

The selection and deployment of enterprise and desktop applications is often guided by requirements, standards, and recommendations such as those imposed by:

- Professional Associations such as EDUCAUSE
- University and Information Technology Strategic Plans
- University Procurement Policies and Standards
- IETF standards for messaging; e.g. SMTP, POP3, IMAP
• Widely accepted higher education practices such as Oracle Calendar and Microsoft Exchange
• Extensible Markup Language and Style sheets; e.g. XML, XSL, CSS
• Open Web Application Security Project (OWASP)
• Accessibility Standards.
• Java Servlet specification (JSR-154)
• Java Portlet specification (JSR-168)
• Separation of business model and related logic from the means used to present the application to the user; i.e. MVC design pattern for web applications is a best practice.

Data
The use and protection of institutional data is described in the data classification policy. This policy establishes uniform data management standards, identifies the shared responsibilities for assuring data integrity, and works to ensure that data is used to meet the needs of the university. The protection of data is often prescribed by requirements, standards, and guidelines such as those imposed by the following:
• Gramm-Leach-Bliley Act
• Family Educational Rights and Privacy Act (FERPA)
• Health Insurance Portability and Accountability Act (HIPAA)
• Credit card industry certifications and practices such as Payment Card Industry’s data

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law
University Policy #3502 IT Infrastructure, Architecture, & Ongoing Operations
University Policy #3505 Information Technology Security Policy
IT Standards

E. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>ITAC/CIO</td>
<td>Created</td>
</tr>
<tr>
<td>October 2009</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2012</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>February 2013</td>
<td>IT Policy Office</td>
<td>Numbering revision</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor updates</td>
</tr>
</tbody>
</table>