Standards and Guidelines for Information Technology Infrastructure, Architecture, and Ongoing Operations

Last revised 12 February 2007

This document describes applicable standards and guidelines for the university's policy on Information Technology Infrastructure, Architecture, and Ongoing Operations.

Introduction

The university selects from among the best and most appropriate of the various national and international standards and practices when determining which course to follow for information technology infrastructure, architecture, and ongoing operations. These decisions are made at discrete intervals in time, typically when a new project begins or when an event occurs that causes the institution to rescan the technology environment and reselect from among the available standards and practices. This document will be updated whenever there is a significant shift of focus in one of the technology or operational domains described below.

A challenge for the university is the need to support a broad spectrum of information technology operations - from traditional administrative infrastructure to the dissimilar needs of high-end, research computing. Distinctions between the purely administrative aspects of higher education information technology and those related to the research and education missions of the institution frequently blur as a single infrastructure is optimized and deployed to support the many different aspects of the university's role in the commonwealth.

Unlike much of industry, institutions of higher education tend to share information and collaborate on joint projects with other colleges and universities. This is especially true in the information technology arena where inter-university collaborations have resulted in significant progress and the deployment of large-scale services. Participation in these joint efforts is often critical as they frequently lay the technology foundation and develop infrastructure that is key to the institution's future competitiveness and its long-term ability to properly support faculty in their research and education activities. These inter-university collaborative projects sometimes help guide technology decisions and at other times represent a set of de facto standards that the institution must follow in order to be able to interoperate with its peers.

Technology Domain Standards

The overarching intent of this document is to describe the technology domains and the standards and guidelines within each domain. It is expected that there will be some overlap between these domains. Technology choices are selected in alignment with the strategic direction of the university.

The needs of existing and planned applications, prevailing and developing industry trends, and the most efficient use of resources form the basis for selecting appropriate

technology standards and operating practices. Open standards and interoperability between discrete technology components are important factors in selecting technologies to meet university needs.

The following technology domains are addressed by this document:

Networking and Telecommunications
Computing, Storage, and Operating Systems
Middleware
Databases
Systems Management
Security
Applications
Data

Standards and guidelines for each of these technology domains are provided in the sections that follow.

Networking and Telecommunications

Institutions of higher education have always been strong contributors to Internet standards and applications, even before the inception of the Internet. Our campus networks are designed as smaller local versions of the Internet with more secure zones implemented where needed and open segments available to foster innovation and support the needs of our researchers. Given this reliance on Internet technology and a requirement to interoperate with the rest of the community, our 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
- 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.

- De facto standard Intel platform that runs Microsoft Windows and a variety of UNIX derivative operating systems
- 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

Our 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 MacOS 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 FCAPS 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 17799 - 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, 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
- Calendaring and scheduling
    - Widely accepted higher education practices such as Oracle Calendar and Microsoft Exchange
    - Promote the further development and use of open standards such as iCal for calendaring to the extent such standards meet the needs.
- Extensible Markup Language and Stylesheets; e.g. XML, XSL, CSS
- Open Web Application Security Project (OWASP)
- Accessibility standards such as Section 508 of the Rehabilitation Act and W3C Guidelines
- 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 protection and management policy. This policy establishes uniform data management standards, identifies the shared responsibilities for assuring data integrity, and works to ensure that data are 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 security standards

Acronyms

Expansion for most acronyms used in this document.

- AIX — **Advanced Interactive eXchange**
- ANSI — **American National Standards Institute**
- API — **Application Programming Interface**
- ATM — **Asynchronous Transfer Mode**
- CIFS — **Common Internet File System**
- CSS — **Cascading Stylesheet Specifications**
- EIA — **Electronic Industries Association**
- IEEE — **Institute of Electrical and Electronics Engineers**
- IETF — **Internet Engineering Task Force**
- IMAP — **Internet Message Access Protocol**
- ISO — **International Standards Organization**
- JDBC — **Java Database Connectivity**
- JSR — **Java Specification Request**
- LDAP — **Lightweight Directory Access Protocol**
- MIME — **Multipurpose Internet Mail Extensions**
- MVC — **Model-View-Controller**
- NAS — **Network Attached Storage**
- NFS — **Network File System**
- OWASP — **Open Web Application Security Project**
- POP3 — **Post Office Protocol, Version 3**
- POSIX — **Portable Operating System Interface**
- RSA — **Rivest, Shamir, Adleman**
- S-MIME — **Secure Multipurpose Internet Mail Extensions**
- SAML — **Security Assertion Markup Language**
- SAN — **Storage Area Network**
- SANS — **SysAdmin, Audit, Networking, and Security**
- SASL — **Simple Authentication and Security Layer**
- SCSI — **Small Computer Systems Interface**
- SMTP — **Simple Mail Transport Protocol**
- SQL — **Structured Query Language**
- SSL — **Secure Sockets Layer**
- TIA — **Telecommunications Industry Association**
- TLS — **Transport Layer Security**
- W3C — **World Wide Web Consortium**
- XML — **eXtensible Markup Language**
- XSL — **eXtensible Stylesheet Language**
- z-OS — **"Z" Operating System from IBM**