WUSTL Enterprise Architecture Principles

Overarching Enterprise Architecture Principles
Principles are simple statements of values that inform and support the way an organization fulfills its mission. Enterprise architecture principles are intended to guide IT decision-making processes, serving as a base for IT architectures, development, policies, and standards.

1. Broadly applicable.

   **Statement:**
   WUSTL’s Enterprise Architecture applies to all aspects of information technology at WUSTL.

   **Rationale:**
   In the WUSTL environment, a consistent framework for information technology promotes better results.

   **Implications:**
   - This applies to all WUSTL systems, data, and infrastructure. Campus-wide, mission critical solutions will be subject to enterprise architecture review and, where deemed appropriate, will require ITPC approval.

   **NOTE:** The enterprise architecture review is NOT an audit. Rather, the purpose of the review is to help the project team leverage the existing architecture and common services, proactively identify the risks to a project, understand the university-wide context in which the proposed solution is to operate, and provide input on how WUSTL’s architecture may need to be modified.


   **Statement:**
   WUSTL’s information systems must support the university’s mission, vision, strategies, and plans.

   **Rationale:**
   Information Technology has the most value when closely aligned with WUSTL’s strategic plans and other university-level direction, concepts, and objectives.

   **Implications:**
   - Architectures will be generated with a specific purpose and for a specific audience to ensure they meet the expectations and needs of its intended stakeholders. WUSTL will not implement technology simply because it is available.

3. Maximize benefit.
Statement: Architectural decisions will maximize the overall benefit to WUSTL.

Rationale: Architectures are designed to provide long-term benefits to the enterprise. Decisions must balance multiple criteria based on business needs.

Implication:
• Criteria used to prioritize may include available funding, governance, and the knowledge, skills, and abilities of WUSTL’s faculty and staff, and may receive different emphases in different situations.

4. Reusability of components.

Statement: WUSTL’s Enterprise Architecture will be built on reusable, loosely coupled modular components.

Rationale: Reusable components provide opportunities to reduce IT development costs and time by leveraging investments in existing systems. Modular components improve system’s ability to adapt to changing requirements.

Implication:
• Loosely coupled modular components must be archived, documented, and searchable for ongoing support and future use.

5. Leverage investments.

Statement: All systems will leverage existing and planned components, enterprise software, management systems, infrastructure, and standards.

Rationale: WUSTL has invested heavily in a number of processes, technologies, infrastructures, and standards. Therefore, to maximize WUSTL’s return on investment, all proposed systems should leverage existing systems as much as possible.

Implication:
• Considering how to leverage or reuse investments is applicable to all technology domains.
• Advocates of proposed solutions should first determine how they might be completed using existing services, modules or systems.
• Searchable repositories and a commitment to populate them are needed for this to be possible.


Statement: System designs, standards, and practices should make university information available to appropriate audiences while protecting information the university controls in accordance with legal, contractual, and ethical requirements for information security and use.
Rationale:
Information is a vital institutional resource whose value is enhanced when used appropriately and diminished when misused, misinterpreted, or when access is unnecessarily restricted.

Implication:
• While providing access to, and safeguarding the integrity of university information is a shared university responsibility, information stewards are responsible for classifying the information in their units and for the processes that generate, distribute, share, and receive university information.
• Decisions about providing access to information are based on the classification and the value of the assets, which is determined by its use, sensitivity, and importance to the university, in compliance with university policy, state, and federal regulations, and other obligations regarding privacy and confidentiality of information.

Business Architecture
Business Architecture documents and models an organization’s policies, processes, work activities, artifacts, and assets. Specifically, Business Architecture answers the following questions concerning WUSTL’s organizations and processes:

• What do they do?
• Who does it?
• Why do they do it?
• How do they do it?
• When do they do it?
• Where do they do it?

Business architecture is a part of enterprise architecture that creates a “blueprint of the enterprise that provides a common understanding of the organization, and is used to align strategic objectives and tactical demands.”

To create the blueprint, BA uses models to represent an organization to help executives answer commonly asked questions: who, what, where, when, why, and how. The answers are then used to develop plans and implement business decisions.

Business architecture may include the following:

- Organizational strategy
- Current initiatives and projects
- List of customers
- Information
Principles of business architecture guide developers’ approaches to technology products created for a business unit.

1. **BA is about the business and not IT.**

   **Statement:**
   Business architecture is not constrained by technology.

   **Rationale:**
   Business architecture describes the business model independent of its supporting technology and provides the foundation for the analysis of opportunities for automation.

   **Implication:**
   - Eliminate technology constraints when defining business architecture and ensure automated processes are described at the business process level for analysis and design.
   - University units and IT organizations must have a common vision of both a unit’s business functions and the role of technology in them.
   - The university unit and IT have joint responsibility for defining the IT needs and ensuring that the solutions delivered by the development teams meet expectations and provide the projected benefits.

2. **BA is about examining processes.**

   **Statement:**
   Business processes must be documented, analyzed, simplified, or otherwise redesigned for optimization and efficiency before automating them.

   **Rationale:**
   Opportunities for increasing efficiency, effectiveness, and quality can be identified and realized through simple and flexible business processes.
Implications:

- Analyze business processes to simplify, integrate, eliminate redundancy, and increase efficiency.
- Identify common business processes for reuse and design business processes to enable business agility.

3. Enterprise business processes drive architecture.

Statement:
The business processes of the enterprise must drive the architecture of any individual system or solution.

Rationale:
Solutions that do not align with the processes of the enterprise inevitably result in inefficiencies, confusion, and poor performance of both systems and processes.

Implications:

- The architecting, designing, and building of solutions must be considered within the context of the enterprise’s business processes, policies, and best practices.
- While BA provides the context for software development to assure that software development efforts are aligned with the organization’s strategic goals and tactical priorities, it does not provide the level of detail required to initiate a software development effort.
- BA is not meant to be a replacement for the analysis and design deliverables that precede software development.

4. BA is reusable.

Statement:
BA provides a foundation for future analysis and decision-making and can be used as a starting point for future efforts.

Rationale:
BA is not a one-time analysis of a business environment; it also provides a foundation for future analysis and decision-making.

Implications:
• Identify opportunities for common components and implement them in such a way that there is an opportunity for reuse by another department, program, or unit of the university.
• Provide a mechanism for units across campus to learn about and access the “reusable” components.
• Use the existing business architecture description and deliverables as a starting point for future efforts, unless an organization has fundamentally changed.

Information Architecture
Information/Data Architecture documents and models both key information assets and the applications that use them to enable business processes, and shows how applications and information together support the enterprises functions. The information architecture also specifies which parts of the business process are supported by each application and where each type of data is stored and managed.

WUSTL’s Information Architecture is comprised of two sub-architectures:

• **Information and Data Architecture** – Using data models, the Information and Data Architecture identifies the information and data WUSTL manages to perform its mission. For example, access and distribution models identify WUSTL enterprise data stores and information flows.
• **Applications and Systems Architecture** – represents the IT application portfolio, the models for how applications are integrated, and identifies the business systems that enable and support the execution of WUSTL’s business processes.

Information Architecture

1. **Information is a university asset.**

   **Statement:**
   Information is an asset that has value to the enterprise and needs to be managed and treated much like a physical asset.

   **Rationale:**
   Information is a corporate resource; it has real, measurable value. In simple terms, information is used to aid decision-making, and accurate, timely information is critical to accurate, timely decisions. We must also carefully manage information to ensure that we know where it is, can rely on its accuracy, and can obtain it when and where we need it.

   **Implications:**
   • Ensure that all organizations understand the relationship between the value of information, sharing of information, and accessibility to information.
• Make the cultural transition from "information ownership" thinking to "information stewardship" thinking.
• Measure and document the current value, risk, and cost of the asset as you would any physical enterprise asset, such as property or equipment.
• Recognize that the ease of moving and copying information is a hidden source of significant inefficiencies and cost in terms of information management.
• Make information accessible to its authorized end users without wasting resources.

2. **Information management is everyone’s business.**

   **Statement:**
   All organizations in the enterprise participate in information management decisions needed to accomplish business objectives.

   **Rationale:**
   Information users are the key stakeholders or customers in the application of technology to address a business need. In order to ensure that information management is aligned with the business, all organizations in the enterprise must be involved in all aspects of the information environment.

   **Implications:**
   • To operate as a team, every stakeholder or customer will need to accept responsibility for developing the information environment.
   • Commitment of resources will be required to implement this principle.
   • The information architecture must encourage management and sharing of data to maximize value at the lowest cost to the university.

3. **Information is accessible and shared.**

   **Statement:**
   Users have access to the information necessary to perform their duties; therefore, information is appropriately shared across enterprise functions and organizations.

   **Rationale:**
   Wide and timely access to accurate information improves the quality and efficiency of enterprise decision-making. Simply put: it is less costly to maintain timely, accurate information in a single application, and then share it, than it is to maintain duplicate information in multiple applications.

   **Implications:**
• Shared information will result in improved decisions since we will rely on fewer sources (ultimately one virtual source) of more accurate and timely information for all of our decision-making.
• Electronically shared information will result in increased efficiency when existing information entities can be used to create new entities without re-keying. Staff time is saved and consistency of information is improved.
• Information needs to be classified in accordance with the security principles of the organization to determine levels of access by faculty, employees, contractors, vendors, partners, suppliers, students, general release, etc.
• To enable information sharing we must develop and abide by a common set of policies, procedures, and standards governing information management and access for both the short and the long term.
• Access to information does not constitute understanding of the information; personnel should take care not to misinterpret information.
• Access to information does not necessarily grant the user access rights to modify or disclose the information. This will require an education process and a change in the organizational culture, which currently supports a belief in “ownership” of information by functional units.

4. **Value and risk determine information classification.**

**Statement:**
An information asset’s classification is determined by its value and risk.

**Rationale:**
A fundamental understanding of the value of an information asset to the business and the business risk if it is exposed, corrupted, or lost is essential to determining the appropriate strategies and investments to make for protecting and managing it.

**Implications:**

• Enterprise information/data standards should be identified when the value of commonality across WUSTL and interoperability with other information systems exceeds the value of uniqueness.
• Information/data should be maintained in a separate data layer decoupled from applications.

5. **Information stewards are accountable.**

**Statement:**
Information stewards are formally assigned accountability for establishing and enforcing the
information policies that govern the access, security, quality, and classification of information assets within their domain of responsibility.

**Rationale:**
One of the benefits of an architected environment is the ability to share information (e.g., text, video, sound, etc.) across the enterprise. As the degree of information sharing grows and business units rely upon common information, it becomes essential that policies and decisions about information within their stewardship are made by the information steward.

**Implications:**
- Real stewardship dissolves information "ownership" issues and allows the information to be available to meet all users' needs. This implies that a cultural change from information "ownership" to information "stewardship" may be required.
- Stewards must have the authority and means to manage the information for which they are accountable and be responsible for meeting quality requirements levied upon the information for which the trustee is accountable.

6. **Enterprise information/data requires primary information/data sources.**

**Statement:**
All enterprise information/data will have an authoritative, official, primary source that is the location for all Create, Update, and Delete actions.

**Rationale:**
For enterprise information/data to be managed effectively, there can be only one primary source for each information/data element. Otherwise, inconsistent and erroneous information/data may result.

**Implications:**
- When the value of commonality across WUSTL and interoperability with other information systems exceeds the value of uniqueness, enterprise information/data standards should be identified.
- Data should only be collected once electronically within a single interface and then shared across systems to provide a “single version of the truth”.
- Information and data management will be looked at from an enterprise perspective.
- A master data approach needs to be adopted and implemented to manage the lifecycle of shared data across the organization.
7. **Use common information vocabulary and definitions across the enterprise.**

   **Statement:**
   Information is defined consistently throughout the enterprise, and the definitions are understandable and available to all users; information architecture needs to be metadata driven.

   **Rationale:**
   The information that will be used in the development of applications must have a common definition throughout the enterprise to enable sharing of information. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange information.

   **Implications:**
   - A comprehensive approach for metadata management is the key to reducing complexity and promoting re-usability across the enterprise. A metadata-driven approach makes it easier for users to understand the meaning of data and to understand the lineage of data across the environment.
   - Whenever a new information definition is required, the definition effort will be coordinated by an “enterprise information administrator” and reconciled with the university "glossary" of information descriptions.

8. **Information quality needs to be measured.**

   **Statement:**
   Information quality is neither abstract nor qualitative and should be measured in absolute terms.

   **Rationale:**
   Information quality is relative to the purpose to which it is to be applied. Decision makers need to not only have access to information; they also need to understand the timing, reconciliation, and accuracy of that information. Research shows that the quality of information is more important than the volume of information.

   **Implications:**
   - Most enterprises underestimate the extent, severity, and business implications of information quality problems. A pragmatic effort needs to be made to appreciate the types of problems that can exist and reveal them before plunging into data cleansing and integration efforts.
• Additional polices and procedures may need to be developed in order to implement this principle.

9. **Use an integrated information security approach.**

**Statement:**
Security best practices will be integrated throughout the entire software development lifecycle.

**Rationale:**
By embedding security and privacy throughout the software development lifecycle, the total cost of development is decreased, overall quality is improved, and security vulnerabilities are significantly reduced.

**Implications:**

• Design security into information elements from the beginning.
• Approach it in a deliberate, well-defined, procedural manner—not as an afterthought or haphazardly.
• Design and integrate security in alignment with the organization’s “business rules” and the existing regulations that stipulate the safeguarding and the privacy of information.
• Identify and develop security needs at the information/data level as well as the application level to protect information from unauthorized use and disclosure.
• Information security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labeling for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined.
• Systems, information, and technologies must be protected from unauthorized access and manipulation, including inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.
• Open sharing of information and the release of information must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

**Application and System**
Applications and Systems Architecture represents the IT application portfolio and the models for how applications are integrated, and identifies the business systems that enable and support the execution of WUSTL’s business processes.

1. **Applications are aligned with business needs.**
Statement:
Applications will have an identified business owner and technical owner.

Rationale:
Technology is effective only when aligned with business needs. Both technical and business interests will be represented when making decisions.

Implications:

- Applications will have a stated business purpose. If there are multiple business purposes, they will be closely related.
- Architectural decisions will seek to maximize value to the customer.
- Architectural decisions will seek to simplify operations
- Architectural design precedes application development

2. **Enterprise solutions chosen over point solutions.**

Statement:
Enterprise applications will meet broad needs.

Rationale:
Enterprise applications that consider only a subset of needs are unsuitable for enterprise-wide use.

Implications:

- The project and deployment plan will need to consider this up-front. Adequate communication methods will be developed.
- Cross-silo solutions are preferred over duplicative, silo-specific applications, systems, and tools.
- Developers will consider the enterprise impact of a solution’s architecture.

3. **Custom applications are least preferred.**

Statement:
A decision to build custom applications should be made only after an analysis that considers other WUSTL sources and third-party alternatives.

Rationale:
Decisions that are made without considering the alternatives may be expensive and difficult to support. There is no reason to re-invent something that already exists.
Implications:

- Project teams, architects, and system engineers will consider existing technologies before developing new ones.
- An analysis of industry-leading third-party solutions will also be considered.
- Consider "subscription" over purchasing where possible and practical.
- Total Cost of Ownership should be a part of any analysis.

4. Applications are technologically independent.

Statement:
Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.

Rationale:
Applications should be independent of underlying technology to allow for the most cost-effective and timely development, upgrade, and operation.

Implications:

- Application Program Interfaces (APIs) will need to be developed so legacy applications can operate with applications and operating environments developed under the enterprise architecture.
- For Commercial Off-The-Shelf (COTS) applications, there may be limited current choices, as many of these applications are technology and platform-dependent.
- Middleware should be used to decouple applications from specific software solutions.
- Technology independence will require standards that support portability.

5. Applications are easy to use.

Statement:
Applications should be easy to use with the underlying technology invisible to users, so they can concentrate on tasks at hand.

Rationale:
Ease-of-use is a positive incentive for application use. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task.

Implications:
An application should be easy to learn.
Content and navigation will be consistent.
Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability.
Underlying technical implementations should be hidden from users.
User actions should have predictable results.
User interfaces will be as simple and intuitive as possible.
User interfaces will be designed to maximize accessibility (to as wide an audience as possible).
User interfaces will be designed to provide fail-safe features to protect users from unintended consequences of actions.

6. Applications are easy to support and maintain.

Statement:
Enterprise applications should be easy to support, maintain, and modify.

Rationale:
Enterprise applications that are easy to support, maintain, and modify lower the cost of support, and improve the user experience.

Implications:

- Enterprise applications will be well documented. Documentation standards need to be developed that include architecture, design, and run book information.
- Applications have a limited life span—end of life should be anticipated and plans for replacement developed.
- Experimental or early release technologies will not be used unless they are critical to competitive advantage.
- Applications will have the following characteristics:
  - **Flexible.** Applications will be architected to minimize the costs of future changes.
  - **Extensible.** Applications will provide "hooks: (i.e. SOA APIs) that allow functionality to be extended in the future.
  - **Highly Available.** All applications will publish availability targets that have been agreed upon with the business.
  - **Interoperable.** Applications will be interoperable.
  - **Minimal Feature Set.** Features add complexity and should be kept to a minimum (avoid bells and whistles and systematic handling of improbable exceptions).
o **Monitored and Measured.** Applications will be built to support monitoring and measurement.

o **Scalable.** Applications will be designed to handle higher loads when allocated more resources.

7. **Build for reusability: Service Oriented Architecture (SOA).**

   **Statement:**
   Applications should be assembled, in part, from reusable components or services.

   **Rationale:**
   Reusable components lower cost of subsequent application development.

   **Implications:**
   - Developers should create new components as part of the implementation of new functionality.
   - Services are to be defined around business functions, not remote procedural calls.
   - Separation of Concerns: It will be possible to change a component with minimal impact to other components.
   - Services will be loosely coupled (producers loosely coupled from consumers), self-describing, designed to maximize enterprise-wide reuse, discoverable, hide their underlying implementation details, stateless, autonomous, have significant control over the functions they provide, and finally, have a defined security policy.

8. **Plan for integration.**

   **Statement:**
   Enterprise applications will plan for and include known, published mechanisms for integration.

   **Rationale:**
   Better application integration will reduce redundant data entry, will decrease the number of reconciliation problems, and will make accurate data available quickly.

   **Implications:**
   - Application integration is to be planned for and is required in the early project planning process for enterprise applications and is to be included in the project plan and key deliverables such as requirements, analysis, and design.
• Interfaces are to be loosely coupled, backward compatible, self-describing, and offer a low impact to the enterprise if change; when tightly coupled, they are 1) less general and 2) more likely to result in undesired side effects when changed.

• Integration points are to be published.
  o “Public” inputs and outputs of an application must be known, published, and understood to promote open data exchange and interfaces for enterprise application integration.
  o Diagrams of connections and data syntax and semantics should be published to promote re-use.
  o “Private” interfaces should not be published or used, as their stability is not guaranteed.

• Open/Industry standards are preferred for enterprise application integration solutions; mechanisms should be language and platform independent.

• Enterprise application integration mechanisms should be as non-invasive to the applications as possible. For instance, data transformation should be done externally from the applications involved. By not adding application integration code to existing applications maintenance burdens and time required for integration projects can be reduced.

• Real-time integration is preferred over batch integration.


Statement:
Applications that support open standards are preferred. Developers of community or enterprise applications will comply with all WUSTL standards in effect at the time. This principle applies to internal or outsourced development and to third-party software.

Rationale:
Compliance with standards will improve overall quality of applications. Therefore, when third-party software does not fully comply with WUSTL standards, a balanced evaluation is necessary.

Implications:

• WUSTL standards need to be published and made available to the developers community.
Technology Architecture

Technology Architecture represents WUSTL’s technical infrastructure and the specific hardware and software technologies that support WUSTL’s information systems. The Technology Architecture consists of the following domains:

- **Platform** – consists of the combination of software, middleware, hardware infrastructure and development frameworks that enable the development, deployment, operation, integration and management of applications.

- **Systems Management** – consists of the technical tools used to collect and analyze data that measure WUSTL system performance to improve system availability, performance, and reliability.

- **Networks** – consist of the technical elements required to provide data and Internet connectivity and communication internal and external to WUSTL.

**Platform**

1. **Platforms for mission-critical, enterprise-class solutions are CIO approved.**

**Statement:**
Mission-critical, enterprise-class solutions are to run on CIO-approved and supported platforms.

**Rationale:**
Because of the inherent risks to the University of developing, deploying, integrating, and managing applications on non-secure and non-stable platforms, it is critical that these be vetted and approved by the CIO.

**Implications:**

- CIO-approved platform standards and guidelines need to be developed.
- Because of the university’s investment in centralizing the expertise and resources required to provide and manage mission-critical, enterprise-class applications in OIT, OIT will be the preferred provider of platforms for this purpose.
- Where external platform providers can provide similar or better services at lower cost, they will be considered.
- Platforms can be hybrid—partly provided by OIT and partly provided by external vendors.
- Platforms, whether OIT-provided or not, are to be highly scalable, reliable, and deliver necessary performance.
• OIT will leverage strategic relationships with other businesses and vendors to facilitate building and evolution of IT architecture.

2. Platforms are available through self-service.

Statement:
The campus community can request access to enterprise platforms via an online order fulfillment process.

Rationale:
The process to deploy approved university systems onto these platforms should be well-documented and simple to use.

Implications:

• Members of the campus community can obtain enterprise platforms from OIT without a formal project.
• Platforms are well-documented, well-supported, and available to be used, much like other platforms in the industry by providers like Amazon.com.
• New systems, or upgrades to existing solutions that require additional customizations should request access to engineers early in the discovery process to identify requirements, timelines and key deliverables.

3. Platforms are customizable.

Statement:
Basic server platform configurations are pre-configured, well documented, and “ready to use”. These platforms are readily available to approved members of the campus community. Users can request additional features or “custom” (non-standard) versions of platforms.

Rationale:
Enterprise platforms are flexible and easily customized. Documentation is readily available and informs the user on how to use it, how to customize it, and how to make and save changes.

Implications:

• Approved users, or consumers of IT systems and platforms, can access, download, and customize standard configurations.
• Once installed, users can make enhancement requests, save modifications to, and even share alternate versions.

4. **Platforms are scalable.**

**Statement:**
IT platforms are capable of growing in capacity to match the dynamic demands of applications and systems. IT platform interfaces will be loosely coupled, backward compatible, self-describing, and offer a low impact to the enterprise if changed. Like applications, platforms are interoperable and have published API’s and established interfaces for integration.

**Rationale:**
Loosely coupled interfaces result in solutions that are more general and require less effort to change when necessary.

**Implications:**

• Elastic, scalable, and flexible.
• Well-documented APIs are necessary.
• “Public” inputs and outputs of an application must be known, published, and understood to promote open data exchange and interfaces for enterprise application integration.
• Diagrams of connections and data syntax and semantics should be published to promote re-use.
• The IT platform architecture and related components built upon it should be viewed as a set of independent services that can be combined to provide a solution.

**System Management**

1. **Enterprise systems management is centrally provided.**

**Statement:**
Systems Management solutions are expected to be centrally provided and include monitoring and management of key functions.

**Rationale:**
System providers need a complete view of all the components that support enterprise applications, including those outside of OIT, so they can provide stable and reliable services to their users.
Implications:

- All systems and IT services should have meaningful performance measurements on which to base reviews and decisions for future direction and improvement needs.

2. Systems management is part of every solution design.

Statement:
As a critical element to a “completely finished solution”, systems management is to be designed into the solution early in the design process.

Rationale:
Without adequate systems management, service providers cannot be proactive in avoiding user problems with their solutions.

Implications:

- Solutions should be designed to be autonomic, self-operating, self-monitoring/analyzing, self-protecting, and self-optimizing.
- In the event of an error condition that cannot be self-corrected, systems should be designed to report appropriate events describing the error condition.
- Events regarding a system’s availability, performance, etc., should also be identified and reported for each system.
- Systems management must not only resolve immediate issues, it must also facilitate the organization’s ability to continuously improve its products and services.

3. Systems management tools are self-service.

Statement:
Systems Management tools will provide a simple self-service interface that allows providers and users to check system, network, or problem status.

Rationale:
Users and administrators should have access to system, network, or problem status without having to call the Help Desk or NOC. This capability would assist them in their own troubleshooting and service level processes. Best practices also recommend allowing users to check the status of their own problems.

Implications:
• Systems should be designed to provide support and operational access tools/panels that allow controls for diagnostics, reset-restart-restore, performance measurement, and fulfillment—in short, functions that require technician interaction. This access provides for secure, limited human interface when needed.
• Self-reporting is preferred.
• Monitoring information should be available through web service APIs.

Network
Key to the university infrastructure is the network. We believe that the network should be open, easy to access, and adequate in capacity to deliver information quickly and securely.

1. **Networks are centrally provided and managed.**

   **Statement:**
   The Office of IT ("OIT") operates both enterprise wired and wireless networks.

   **Rationale:**
   OIT network engineers are expertly trained and uniquely qualified to develop, operate, and maintain the network. Much like platform architecture, this centralized approach will reduce total cost of ownership to the university, minimize complexity, increase reliability, and improve performance.

   **Implications:**

   - OIT engineers will keep WUSTL networks current with hardware and software providers’ updates and releases.
   - The network will meet the network service level objectives agreed upon by OIT management and campus users and external partners. The network management systems will have the capability to measure and report end-to-end network service level statistics.
   - Service Level Agreements (SLAs) will be documented and network statistics and SLAs will be published to the end-user community as needed, to ensure network resources are aligned with business needs.
   - 24x7 support is available for users to call and receive help with WUSTL network.

2. **Networks are standards-based.**

   **Statement:**
   WUSTL-hosted networks refer to both wired and wireless communications and adhere to industry standards for communication protocols, hardware, and security.
Rationale:
Adherence to proven and adopted industry standards for network architecture will improve the use, operation, and management of wired and wireless networks on campus. This approach ensures the best possible service for network users, reduces unnecessary costs, and maintains security.

Implications:

- WUSTL networks will use open industry standards and leverage existing best practices.
- Open, rather than proprietary, systems will be used where feasible and cost-effective.
- OIT engineers will minimize the number of platforms and systems supported.
- WUSTL will need to have experts assigned to track evolving trends and improvements in network security.
- WUSTL networks will leverage strategic relationships with other businesses and vendors to facilitate the building and evolution of IT architecture.
- Improvements and upgrades to infrastructure will need to be planned, resourced, and communicated to sponsors and users.
- Audits and reviews will be necessary to monitor compliance.

3. Networks are readily accessible.

Statement:
Users (visitors, students, faculty, staff, etc.) should be able to quickly and easily access WUSTL networks.

Rationale:
With the emergence of cellular data networks like AT&T’s LTE network, users can easily, if not seamlessly attach devices. The remote access network will consist of a defined set of technical options for the delivery of reliable, cost-effective, secure, and ubiquitous remote access capabilities.

Implications:

- Network tools like Virtual Private Network clients, must be issued to users wishing to access secure resources remotely.
- It is not necessary to register devices, scan devices, etc.
- WUSTL provides users the ability to access the network remotely.
Remote access will be designed and provisioned for use enterprise-wide.

4. **Networks are fast.**

   **Statement:**
   WUSTL networks will provide application response times acceptable to support the business need, and cost effective bandwidth to satisfy the current and future networking needs of its users. The WUSTL network should meet the requirements of its users and provide the ability to deliver information.

   **Rationale:**
   The network will not be overbuilt and will be efficient. The network should also be able to accommodate future networking needs. In conjunction with response time, throughput ensures that information is adequately delivered.

   **Implications:**
   - Network performance is measured in terms of “response times” which should always be monitored and optimized.
   - The network should be designed to provide appropriate application response times at a reasonable cost.

**Information Availability and Security**

The three common goals of Information Availability and Security are: Availability, Confidentiality, and Integrity. Enterprise business priorities and risk are considered and evaluated from the beginning of potential IT endeavors rather than as an afterthought.

**AVAILABILITY** - For any information system to serve its purpose, the information must be available to authorized individuals and systems when needed.

**CONFIDENTIALITY** - Confidentiality means that disclosure of information to unauthorized individuals or systems is prevented.

**INTEGRITY** - In Information Security, integrity means that data is accurate and cannot be modified undetectably by unauthorized individuals or systems.

1. **Alignment with security policies.**

   **Statement:**
   Security policies should drive the implementation of business and technical security
controls.

**Rationale:**
Business and technical security controls are put in place to enforce compliance with existing security policies.

**Implications:**

- There should be a way to monitor and measure the security compliance of each IT system.
- Information stewards review security compliance regularly.

2. **Least privilege.**

**Statement:**
The principle of least privilege requires that, in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

**Rationale:**
Least privilege is an important design consideration for the protection of data and functionality from faults and malicious behavior. Benefits include better system stability, better system security, and ease of deployment.

**Implications:**

- User accounts should be given only those privileges essential to that user’s work.
- Applications should only acquire information necessary for their operations.
- Applications should not store information that is readily available from online sources.

3. **Adequate security controls.**

**Statement:**
Security controls will be selected on the basis of a risk analysis and risk management decision; will provide only the required level of protection, alerting, and response; will prefer the ability to be applied uniformly across the WUSTL enterprise (standardized); and will be modular so that they may be removed or changed as the system and enterprise risk profile changes.

**Rationale:**
By providing only the required levels, we will not impose unreasonable constraints or operate in a manner that causes unreasonable response.

Achieving a standards-based environment will reduce operational costs, improve interoperability, and improve supportability.

It is prudent to minimize the interdependence of controls so that they can be easily interchanged or modified.

**Implications:**

- The appropriate security officer and committees will need to be involved.
- Controls should default to the most secure condition.
- Controls should have the capability to be shut down gracefully and restored automatically to the conditions prior to shut down.
- The CIO, acting as primary sponsor, should be apprised of any changes or recommendations.
- Consideration for industry-proven standards will be applied in the requirements phase of project definition.
- The implementation of controls should be aligned closely with operations’ personnel, and adhere to approved procedures for change management.
- Protection and response decisions should come from the appropriate information stewards.
- The implementation of controls should be aligned closely with operations’ personnel and adhere to approved procedures for change management.

4. **Security planning.**

**Statement:**
Information systems security will be built into systems from their inception rather than “bolted on” after system implementation.

**Rationale:**
The cost and complexity of adding security controls to a system after it is already in production is significantly greater. Controls should provide only the required level of protection, alerting, and response.

**Implications:**

- Preliminary architectural plans will address security consideration before systems are purchased or developed internally.
- Early design work will need to include the definitions of how and where controls will be implemented.
• Security officers and appropriate committees will review any large-scale, enterprise-wide impact to security modifications.
• Protection and response should align with the appropriate data stewards.

5. Security measurement.

Statement:
All functional security requirements that define the “what” a system or product does will have associated assurance requirements to define “how well it does it.”

Rationale:
Security controls can be reviewed or audited through some qualitative or quantitative means to ensure that risk is being maintained at acceptable levels.

Implications:
• Documentation will need to be developed to allow approved groups to review and measure the performance of security systems.


Statement:
The architecture will embrace the concepts of compartmentalization and defense-in-depth.

Rationale:
Compartmentalization localizes vulnerabilities, and defense-in-depth establishes a series of imperfect countermeasures.

Implications:
• Compartmentalization concepts will need to be included in both preliminary and detailed designs.
• Management and review of various areas will need to be assigned to the appropriate party.


Statement:
Controls will minimize the need for manual operation.

Rationale:
Manual operation can create vulnerabilities and cause disruption of service due to misinterpretation and misconfiguration.

Implications:

- Automation will be a key requirement in the deployment of each new system.
- Documentation will need to be developed on how to implement these systems.

8. Separation of duties.

Statement:
The designer and the operator of a security control will be independent.

Rationale:
Separation of duties ensures that there is no conflict of interest in the design of security control.

Implications:

- The appropriate roles and responsibilities for operation and implementation of security systems will need to be clearly defined and communicated.