Principles

Architecture Principles provides foundation in following areas

- **Architecture Principles** articulate the fundamental rules and guidelines used to define the Architecture Strategy.
- **Architecture Principles** ultimately form the basis for making IT decisions regarding the selection, use, and deployment of all IT resources and assets across the enterprise.
- **Architecture Principles** should be clearly related back to the business objectives and key architecture drivers.

Below are the list of principles approved by CUIT Leadership and Columbia University Leadership teams.

**Enterprise Architecture Principles**

*Columbia University Enterprise Architecture - version 0.1 - 2014-12-04*

**Introduction and Background**

Prior CUIT architecture principles date back several years and were created ad hoc by the Technical Architecture Group and others. These TAG principles are revised, enhanced and recast here in light of matured understanding and guidance from TOGAF.

**Business Principles**

*CU-PRIN-BUSI-001: Primacy of Principles*

**Statement**

*These principles of information management apply to all organizations within the enterprise.* For the purposes of this version of the Enterprise Architecture, we define the *enterprise* as Columbia University and *organizations* as all academic and administrative units within the University.
Rationale

The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles.

Implications

- Without this principle, exclusions, favoritism, and inconsistency would rapidly undermine the management of information. This concept was best stated by John Adams as, “a government of laws and not of men.” Massachusetts Constitution, Part The First, art. XXX (1780).
- Information management initiatives will not begin until they are examined for compliance with the principles.
- The Project Review Board (PRB) enforces architecture signoff as part of the Project Management Methodology.
- A conflict with a principle will be resolved by changing the framework of the initiative.
- An annual review will re-validate these principles and adjust as required.
- A formal dispensation process exists to allow and track necessary exceptions.


Statement

The enterprise's Intellectual Property (IP) and individual privacy and academic freedom must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes.

Rationale

A major part of the enterprise's and individuals' IP is hosted in the IT domain. Protecting the personal privacy and academic freedom of the institution's students, faculty, staff, patients, clients and others are core values of the institution and the enterprise must also protect these rights.

Implications

- While protection of IP assets is everybody’s business, much of the actual protection is implemented in the IT domain. Even trust in non-IT processes can be managed by IT processes (email, mandatory notes, etc.).
- A security policy, governing human and IT actors, will be enforced that can substantially improve protection of IP. This must be capable of both avoiding compromises and reducing liabilities.
- Use of technology to implement data integrity and confidentiality will explicitly be architected to protect individual privacy and academic freedom.
- Resources on such policies can be found at the Administrative Policy Library (http://policylibrary.columbia.edu).
- This principle applies to all people that the University serves, including, for example, applicants, clients, patients, and other individuals that the institution serves.

CU-PRIN-BUSI-003: Business Continuity

Statement

Enterprise operations are maintained in spite of system interruptions.

Rationale

As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms.

Implications

- Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities.
- Recoverability, redundancy, and maintainability should be addressed at the time of design.
- Applications must be assessed for criticality and impact on the enterprise mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.
- Refer to the University Business Continuity and Disaster Recovery Policy at http://cuit.columbia.edu/it-policy-summaries.
Service Level Agreements (SLA) and Operating Level Agreements (OLA) will be established to ensure agreed requirements for service availability are met.

**CU-PRIN-BUSI-004: Common Use Services/Applications**

**Statement**

Development of services/applications used across the enterprise is required over the development of similar or duplicative services/applications which are only provided to a particular organization.

**Rationale**

Duplicative capability is expensive and proliferates conflicting data.

**Implications**

- Organizations which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability. This will require establishment of and adherence to a policy requiring this.
- Organizations will not be allowed to develop capabilities for their own use which are similar/duplicative of enterprise-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Data and information used to support enterprise decision-making will be standardized to a much greater extent than previously. This is because the smaller, organizational capabilities which produced different data (which was not shared among other organizations) will be replaced by enterprise-wide capabilities. The impetus for adding to the set of enterprise-wide capabilities may well come from an organization making a convincing case for the value of the data/information previously produced by its organizational capability, but the resulting capability will become part of the enterprise-wide system, and the data it produces will be shared across the enterprise.

**CU-PRIN-BUSI-005: Self Service 7x24**

**Statement**

Users shall have access to common University services via self service, getting what they need when they need it.

**Rationale**

Self service capabilities are the norm for our community which operates around the clock. We minimize delays in service delivery and improve service delivery efficiency through automation.

**Implications**

- Services shall be designed with automated request and fulfillment processes.
- Services that require user authentication and authorization follow University identity management standards, thereby leveraging automated on- and off-boarding.
- This principle has implications related to Principle 3: Business Continuity with respect to evaluating criticality and impact.

**Data Principles**

**CU-PRIN-DATA-001: Data is an Asset**

**Statement**

Data is an asset that has value to the enterprise and is managed accordingly.

**Rationale**

Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.
Implications

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data.
- Stewards must have the authority and means to manage the data for which they are accountable.
- We must make the cultural transition from “data ownership” thinking to “data stewardship” thinking.
- The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise.
- Part of the role of data steward, who manages the data, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality - it is probable that policy and procedures will need to be developed for this as well.
- A forum with comprehensive enterprise-wide representation should decide on process changes suggested by the steward.
- Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level.

**CU-PRIN-DATA-002. Data is Shared**

**Statement**

Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations.

**Rationale**

Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The enterprise holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization.

Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

**Implications**

- To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term.
- For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment.
- We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible. Where available, we strongly prefer open data formats and protocols as we should always endeavor to reuse existing building blocks.
- For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.
- For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the enterprise.
- Data sharing will require a significant cultural change.
- This principle of data sharing will continually “bump up against” the principle of data security. Under no circumstances will the data sharing principle cause confidential data to be compromised.
- Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the enterprise-wide "virtual single source" of data. "Link, don’t duplicate."

**CU-PRIN-DATA-003. Data is Accessible**

**Statement**

Data is accessible for users to perform their functions.

**Rationale**

Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.
Implications

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data.
- Accessibility involves the ease with which users obtain information.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of enterprise users and their corresponding methods of access.
- Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
- Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the organizational culture, which currently supports a belief in “ownership” of data by functional units.

CU-PRIN-DATA-004: Common Vocabulary and Data Definitions

Statement

Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users.

Rationale

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

Implications

- We are lulled into thinking that this issue is adequately addressed because there are people with “data administration” job titles and forums with charters implying responsibility. Significant additional energy and resources must be committed to this task. It is key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community - this is more like a common vocabulary and definition.
- The enterprise must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the enterprise.
- Whenever a new data definition is required, the definition effort will be co-ordinated and reconciled with the corporate “glossary” of data descriptions. The enterprise data administrator will provide this coordination.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted enterprise-wide definitions and understanding.
- Multiple data standardization initiatives need to be co-ordinated.
- Functional data administration responsibilities must be assigned.

CU-PRIN-DATA-005: Data Security

Statement

Data is protected from unauthorized use and disclosure.

Rationale

Appropriate sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of sensitive, confidential and internal information and the protection of individuals’ expectations of privacy and protection of their academic freedom. Existing laws and regulations require the safeguarding of the privacy of data, while permitting appropriate access.

Implications

- In order to adequately provide access to information while maintaining secure information, security needs must be identified and developed at the data level, not the application level.
- All data shall be classified as Sensitive, Confidential, Internal or Public, as defined in the University Data Classification Policy, and protected appropriately.
- Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. Data security must be designed “on the left side” of the development lifecycle flow, not added “on the right” (at the end).
- Endpoints, systems and applications must be classified by the types of data they use, registered and protected to the level appropriate for that data classification, per the University Registration and Protection of Systems and Endpoints Policies.
- Complete information regarding University data security policies may be found in the Administrative Policy Library: [http://cuit.columbia.edu/it-policy-summaries](http://cuit.columbia.edu/it-policy-summaries)
Application Principles

**CU-PRIN-APPL-001: Technology Independence**

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

**Rationale**
Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves. Realizing that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software.

**Implications**
- This principle will require standards which support portability.
- For Commercial Off-The-Shelf (COTS) applications, there may be limited current choices, as many of these applications are technology and platform-dependent.
- Subsystem interfaces will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the enterprise architecture.
- Middleware should be used to decouple applications from specific software solutions.
- As an example, this principle is supported by the use of Java, and future Java-like protocols, which give a high degree of priority to platform-independence.
- This principle may lead to conflict with Cloud SaaS or PaaS which frequently derive their benefit from vendor-proprietary approaches.

**CU-PRIN-APPL-002: Buy Before Build: Cloud First**

**Statement**
When selecting a new application we prefer acquiring Software as a Service (SaaS) or a commercial or open-source off the shelf (COTS/OSOTS) application in favor of building an application. Developing an application in-house should be done only as a last resort after exhausting all alternatives.

**Rationale**
Most business processes we are likely to support are comparable to those used widely. We should be able to apply an existing solution rather than “reinventing the wheel.” Locally-developed application support is costly and does not benefit from the economies of scale found when using an application that has the benefit of a larger customer base. Using SaaS/COTS/OSOTS reduces risk during upgrades and reduces the staff on-boarding and learning curve as they are likely to have used a commonly-available application elsewhere.

**Implications**
- Business process re-engineering may be required in order to align our processes to leading practices.
- Every effort should be made to avoid application customization as such customization has the analogous downside of requiring ongoing maintenance and support and lacks the benefit of development cost that is shared across a wider customer base.
- Consider a common platform service (e.g. workflow tool) as the basis for application development where a direct application is not available.
- When investigating cloud options, prefer SaaS over Platform as a Service (PaaS) over Infrastructure as a Service (IaaS), moving lower in the stack only if a higher-stack service is not available.
- When using open source, contribute improvements made back to the open source product. The extra effort will benefit the community and the institution in the long run.

**CU-PRIN-APPL-003: Service Oriented Architecture (SOA)**

**Statement**
Applications should have a clear separation between business logic (manipulation of data according to business rules) and user interface: a Service Oriented Architecture.
Rationale

By separating the user interface from the business functions performed upon data, we have the flexibility to facilitate mash-ups and flexible user experiences such as multiple UIs for the same application, including web, mobile, and command-line. Applications can invoke other applications to perform services and the potential for real-time data integration across applications is made possible.

Implications

- RESTful APIs are preferred over SOAP when both are available.
- Integration with legacy monolithic applications and their data can be difficult and may require acquiring/developing middleware that makes legacy data available.
- Open authentication/authorization protocols such as OAUTH should be used to meet security and interoperability goals. Web browser-centric protocols are acceptable but may limit applicability to mobile and other non-web applications.
- Prefer SOA web services calls over batch interface files as the means of sharing data. (See "Link, don't duplicate," above).

CU-PRIN-APPL-004: Reuse

Statement

Reuse common building blocks.

Rationale

A fundamental tenet of Enterprise Architecture is the reuse of Architecture and Solution Building Blocks (ABB, SBB). Reuse reduces support complexity and cost.

Implications

- Use established technology standards such as operating systems, app server, database, identity management infrastructure, common application platform services, common software, and common performance and capacity monitoring tools.
- Use the standard application development tool chain of source code version control, provisioning, continuous integration, automated testing, etc.
- Common architecture and solution building blocks will be maintained in the Enterprise Repository.

Technology Principles

CU-PRIN-TECH-001: Control Technical Diversity

Statement

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale

There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements.

Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
- Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place.
We are not freezing our technology baseline. We welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

**CU-PRIN-TECH-002: Interoperability**

**Statement**

Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

**Rationale**

Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.

**Implications**

- Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.
- The existing IT platforms must be identified and documented.