FACULTY LIFECYCLE INITIATIVE PRINCIPLES

The following principles define the general rules and guidelines for all aspects of the Faculty Lifecycle Initiative, reflect a level of consensus among the various elements of the initiative, and form the basis for making future decisions relevant to faculty data.

These principles of the Faculty Lifecycle Initiative apply to all academic units within the university. In order to provide a consistent and measurable level of quality information to decision-makers is for all academic units abide by the principles. Without these principles, the Faculty Lifecycle Initiative would rapidly be undermined by exclusions, exceptions, and inconsistency. Faculty lifecycle projects will not begin until they are reviewed for compliance with the principles. A conflict with these initiative principles will be resolved by modifying the individual project(s).

Business Principles

Principle 1: Maximize Benefit to the University

Statement:

Faculty lifecycle decisions are made to provide maximum benefit to the university as a whole.

Rationale:

This principle embodies "service above self." Decisions related to the initiative made from a university-wide perspective will have greater long-term impact than decisions made from a singular academic unit perspective. Maximum return on investment requires faculty lifecycle decisions to adhere to university-wide drivers and priorities. However, this principle will not preclude any academic unit from getting its job done.

Implications:

- Achieving maximum university-wide benefit will require changes in business process and in the way we plan and manage information. Technology alone will not bring about this change.
- Some academic units may have to make changes in business process for the greater benefit of the entire university.
- Priorities must be established by the entire university for the entire university.
- Faculty lifecycle projects should be conducted in accordance with the university plan. Individual academic units should pursue faculty lifecycle projects which conform to the blueprints and priorities established by the university. We will change the plan as we need to. As needs arise, priorities must be adjusted. A (faculty lifecycle) committee with comprehensive university representation should make these decisions.

Principle 2: Information Management is Everyone's Responsibility

Statement:

All academic and business units in the university participate in faculty lifecycle decisions needed to accomplish business objectives.

Rationale:

Academic units are key stakeholders in the collection, maintenance, and assessment of the faculty information used in all areas of the institution. In order to ensure that faculty information is aligned with university goals and objectives, all academic units of the university must be involved in all aspects of the faculty lifecycle environment. The business managers from across the institution and the technical staff responsible for developing and sustaining the faculty lifecycle environment need to participate as a team to jointly define the goals and objectives of this project.

Implications:

- To operate as a team, every stakeholder will need to accept responsibility for developing the faculty lifecycle environment.
- Commitment of resources will be required to implement this principle.

Principle 3: Roles and Responsibilities of IT and Academic/Business Units

Statement:

IT and academic and business units share accountability and responsibility for the processes, data quality and for defining business requirements. The ITS division is responsible and accountable for the IT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

Rationale:

In order for the Faculty Lifecycle Initiative to be a success, all areas of the university must be willing to collaborate, be transparent, and align expectations with roles and responsibilities. Efficient and effective solutions have reasonable costs and clear benefits when the stakeholders share responsibilities.

Implications:

- When there are more efficient and effective processes, academic and business units willingly change their processes.
- The IT function must define processes to manage business unit expectations.
- Data, application, and technology models must be created to enable integrated quality solutions and to maximize lean processes and data quality.

Data Principles

Principle 4: Data is an Asset

Statement:

Faculty data is an asset that has value to the institution and is managed accordingly.

Rationale:

Data is a valuable resource; it has real, measurable value. The purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most institutional assets are carefully managed, and data should be 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 all departments within the university must 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 executive management and adversely affect decisions across the university.
- 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 institution-wide representation should decide on process changes suggested by the academic or business unit.
- Since data is an asset of value to the entire university, data stewards accountable for properly managing the data must be assigned at the institution level.

Principle 5: Data is Shared and Accessible

Statement:

Academic and business units need access to the data necessary to perform their duties, and data is shared across university functions as necessary for academic and business units to perform their duties.

Rationale:

Accessibility involves the ease with which users obtain information. Timely access to accurate data is essential to improving the quality and efficiency of university 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 university holds a wealth of data, but it is stored in separate incompatible databases and in different formats. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the university to efficiently share these islands of data across the institution.

Shared data will result in improved decisions since we will rely on fewer sources of more accurate and timely managed data for 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 define this shared environment and develop a repository system for storing this metadata to make it accessible.
- 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 university.
- Data sharing will require a significant cultural change.
- Data and information used to support university decision-making will be standardized to a much greater extent than previously. The smaller, departmental capabilities which produced different data (which was not shared among other academic units) will be replaced by university-wide capabilities. A department may make 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 university-wide system, and the data it produces will be shared across the university.
- 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 university-wide “virtual single source” of data.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of institutional users and their corresponding methods of access.
- Access to data does not constitute understanding of the data. Neither does access to data necessarily grant the user access rights to modify or disclose the data. Issues around access and use of data will require an education process and a change in the institutional culture, which currently supports a belief in “ownership” of data by administrative units.

Principle 6: Accountability for the Data is Essential

Statement:

Each academic and business unit is accountable and responsible for its data accuracy, integrity, currency and correct usage of each data element that is updated or used.

Rationale:

One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the university. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee make decisions about the content of data.

Implications:

- Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data ownership to data trusteeship may be required.
- The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.
- It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as "data source."
- It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee.
- Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.
- As a result of sharing data across the institution, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility.

Principle 7: Common Vocabulary and Data Definitions are Essential

Statement:

Data is defined consistently throughout the institution, 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 university to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

Implications:

- A common vocabulary around faculty data 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 university must establish the initial common vocabulary for faculty data. The definitions will be used uniformly throughout the university.
- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the glossary of data descriptions.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted university-wide definitions and understanding.
- Multiple data standardization initiatives need to be coordinated.
- Functional data administration responsibilities must be assigned.

Technology Principles

Principle 8: Security and Privacy of Data Must be Considered

Statement: Appropriate measures are implemented to address the risk of inadvertent disclosure of sensitive (personally identifiable) information.

Rationale:

The University Acceptable Use and Information Policies require the safeguarding of security and the privacy of data, balanced with appropriate access. Pre-decisional (work-in-progress, not yet authorized for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

Implications:

- Aggregation of data that includes classifications of Public, Internal Use, or Restricted data will require means to remove or redact the restricted data, before any results are formally disclosed or otherwise made public. Data owners and/or functional users must determine whether the aggregation will result in an increased classification level. We will need appropriate policy and procedures to handle this review and de-classification. Access to information based on a need-to-know policy will require regular reviews of the body of information.
- In order to adequately provide access to open information while maintaining secure information, security controls must be identified and developed at the data level, not the application level.
- The faculty lifecycle initiative will follow the policies outlined on the Information tiers and sensitivity, http://www.case.edu/its/policy/information_types.html
- Security controls must be designed into data elements from the beginning; they cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. University information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure. Accommodation for emerging threats must also be made in the strategy.

Principle 9: Applications are Easy to Use

Statement:

The underlying technology will be developed with the user experience in mind.

Rationale:

The faculty lifecycle application should be intuitive. The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated outside systems to accomplish a task. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low.

Implications:

- Applications will be required to have a common look and feel and support ergonomic requirements. Hence, the “common look and feel” standard must be designed and usability test criteria must be developed.

- Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.

Principle 10: Systems are Integrated

Statement:

Applications must be able to integrate with other applications.

Rationale:

Duplication of effort and data inconsistency across enterprise systems can be inefficient and costly. However, system integration can be a complex and costly process as well. If integration is required, intent, scope, requirements and rationale must be supplied and evaluated early in the project cycle for each element that needs to be integrated.

Implication:

- Integration of systems will be designed with the faculty and other key stakeholders in mind. Integration between systems will be standardized through web services.
- Data in future applications selected will be easily accessible for integration with other applications.
- Integration of applications and systems will simplify and automate business processes to the greatest extent possible, while avoiding significant changes to current systems.

Principle 11: Plans for Business Continuity are Established

Statement:

A successful faculty lifecycle initiative will result in "system of record" resources and critical business processes need to be protected from outages, interruptions, and system failures. Adequate resources should be devoted to address risks and to enable sufficient confidentiality, availability, and integrity of systems and data.

Rationale:

The faculty lifecycle system will be treated as a critical system by ITS and will follow the university's service level agreement of 99.9% availability.

Implications:

- On Premise:
  - Integrate applications and systems will simplify and automate business processes to the greatest extent possible, while avoiding significant changes to current systems.
  - Design redundancy of hardware systems to minimize the effects of failures and disasters.
  - Plan backups so that backup data is always readily and quickly available. Live mirroring to disk provides the highest level of backup safety and the fastest recovery.
  - Maintain backups off site to guard against disasters.

- Cloud Services:
  - Ensure contract with cloud provider contains provisions for disaster/recovery.