Information Management Model for The University of Scranton

This proposal was made to the Administrator’s Conference in August 2009. The recommended goals for an Information Management Program were endorsed and subsequently the Information Management Advisory Committee (IMAC) was created, its members were appointed as data stewards by their respective Vice President. (February 2012)

Enterprise information management (EIM) “is [both] a technology strategy for organizing, designing, cataloging, and safeguarding structured and unstructured content to maximize its value, usefulness, accessibility, and security...[and]...an organizational commitment to define, secure, and improve the accuracy and integrity of information assets ...” (Gartner Research, 2005).

Conditions driving interest in the value of EIM:

- Need to streamline business processes
- Increase in compliance and regulatory requirements
- Need to manage expanding volume and velocity of information sources
- Need for greater agility (responsiveness to environment) facilitated by access to analytics and single, consistent view of information from across operational areas
- Need to create competitive differentiation in new program offerings, facilitated by data mining, and in customer satisfaction, facilitated by managing relationship information
  (Gartner Research, 2005)

An information management model (also referred to as a program or discipline) consists of tools, policy, people, and metrics; identifying goals and desired outcomes for the program as well as setting the scope of the program are key decisions. The following components currently exist within the University’s Information Management Model:

**Tools:**

- Enterprise Resource Planning systems: Banner
- Content & Record Management systems: My.Scranton (portal), Angel (learning management system), Royal Drive, document imaging, Hannon Hill (website), People Admin (human resources)
- Customer Relationship Management systems: Recruitment Plus (admissions), iDODS and iModules (development), Footprints (information resources)
- Security systems: encryption tools, intrusion prevention and detection systems, anti-malware tools, firewalls, network access controls, and vulnerability scanners
  - Identity & Access Management system (TBD)
- Business Intelligence/Analytics applications: Future Perfect (finance), Advizor Solutions (development), BIQuery, Argos, Excel, locally developed reporting

---

1 Approved by the Administrators’ Conference August 25, 2009
**Policy**

An information management program is managed via a system of information governance. Information governance “establishes the decision rights and accountabilities necessary to encourage desirable behavior in the creation, storage, use, archiving, and deletion of information” (Gartner Research, 2008). Governance “enacts policies and procedures that will guide application development and technology infrastructure; it also provides mechanisms to monitor and enforce metrics, such as accuracy, consistency, and quality, as they relate to information assets;” its scope “spans the life cycle of information from capture and creation through deleting as well as archiving – security, accessibility, and disclosure” (Gartner Research, 2008).

Areas of information governance, groups involved today:

- Information Quality: Data Standards Committee
- Information Security: Information Security Advisory Group
- Information Lifecycle Management: Records Management Advisory Board

These groups advise and guide the development of policies and standards (including selecting tools) and help to set goals and monitor progress. The goals of governance are to ensure that information supports business goals effectively and efficiently.

**People**

**Executive-level**

This group provides sponsorship and strategic direction (sets program goals), communicates support, approves program funding, designates leadership to oversee activities, endorses policies, and reviews program performance – periodically evaluates risk, controls, metrics. (Gartner Research, 2008)

**Data Stewards and Custodians**

Data Stewards should represent each major business function and work in positions where they are empowered to make business process changes and apply resources to address quality issues. They also need the ability to influence how their peers execute business processes to achieve further improvements. These are typically mid-level managers or power users with authority over business processes. The stewardship role should be formalized within the organization, reflecting the time required to perform the role and the authority (both to set goals and be held accountable) needed to carry out the role effectively. Key roles of the data stewards include establishing data classification and data handling practices for their business function. The primary governing body for information issues should be comprised of the data stewards and staff in key information support roles.
**Data Custodians** – in business units that are responsible for managing large volumes of information (admissions or registrar’s office for example), we may also want to identify staff who function as data custodians. Custodians generally perform the following tasks:

- Implement and document data standards in their operations
- Assure reliable data collection processes and archive data on standard cycles
- Implement and document validity checks on applications that capture, update, extract, transfer, load, or report critical data; measure data quality and report erroneous data
- Implement and document access procedures to provide data protection
- Implement backup and recovery procedures that protect data integrity
- Provide accessible, meaningful, and timely data, identifying collection and modification dates and procedures (People, Processes, and Managing Data, 2004)

**Information Resources Staff**

The Chief Information Officer (CIO) is responsible for providing the framework — including structuring the information technology architecture and providing appropriate tools, funding, and staffing — to support an effective information management program. The CIO provides leadership to mitigate risks to the confidentiality, integrity, and availability of University information assets. In consultation with the Information Security Manager and Deputy CIO, determines when public disclosure of information breaches must be made.

The Information Security Manager coordinates the development and maintenance of policies and plans that help to protect the University’s information and technology systems. The manager monitors the regulatory environment to help assure that the University remains in compliance with applicable laws. The manager also monitors and advises on the security posture of the University’s information systems, and detects, contains, and coordinates response to security incidents.

Information technology staff serve in the following roles that support the management of University information: 1) as consultants, providing guidance on the development of policies and practices for accessing and securing data; 2) as information architects, providing data models based on the steward’s specifications; 3) as enablers, helping to identify and make appropriate tools available; and 4) as application administrators, managing and maintaining the selected tools.
**Metrics**

The establishment of metrics is recommended in order to create a mechanism to monitor progress/performance of the information management program. Metrics are derived from program goals in the areas of data quality, security, and lifecycle management.

**Steps Proposed to Develop an Information Management Model at the University of Scranton**

- Establish goals for an information management program (suggested goals below)
  - Develop information management practices that will support and cultivate more efficient work environments.
  - Enable offices and individuals to more effectively manage their information assets.
  - Enhance access to data and provide tools and procedures for consistent reporting and analysis across operational areas.
  - Facilitate access to information to improve customer relationship management practices.
  - Work to ensure the security and privacy of data.

- Establish an information governance system that incorporates existing groups into a single Information Management Advisory Committee

- Formalize the data stewardship and custodian roles in the organization (ideally in job descriptions)

- Establish measures for monitoring progress

**Resources**


Gartner Research:

- Business Drivers and Issues in Enterprise Information Management (2005)
- Governance is an Essential Building Block for Enterprise Information Management (2008)