Haverford College
Data Management Principles
Approved by Senior Staff 6/21/2013
Approved by President Daniel Weiss 7/1/2013

Data collection and management are critical to the success of the College's educational mission. Capturing reliable, high quality data; ensuring broad but appropriately secure access to those data; and providing sophisticated tools and techniques to enable the analysis of those data will allow the College to serve its students, alumni, and institutional stakeholders most effectively. "Data" in this instance refers to: any operational information, current or historical, about College stakeholders (students, faculty, staff, alumni and friends, members of the Corporation and Board of Managers, benefactors and supporters); academic, co-curricular and other programs; institutional finances, operations, and assets; College policies and practices; and all information related to evaluations, assessments, planning exercises, and strategic plans. The data discussed herein do not include academic research, scholarship, course materials, and other forms of intellectual property.

Haverford College follows these data management principles:

1. College data are a shared institutional asset, and individual offices are stewards of that data.

2. The College embraces collaborative and coordinated data collection, and appropriate data sharing to maximize institutional effectiveness.

    a. Data stewards have specific responsibilities for collecting, maintaining, securing, and appropriately sharing data within their purview and systems. (See Appendix I for additional detail.)
    b. The College has a process to resolve questions about appropriate access to data and the sharing of data.

        Data stewards who are unable to determine appropriate access to data or the sharing of data may refer the matter to the Senior Staff member(s) to whom they report for resolution. As with all administrative matters, the President may make a final determination.
    c. IITS is responsible for managing policies and protocols related to centralized and network data storage, security, and access.
    d. The College supports on-going employee technology training.

3. The College and its data stewards abide by all relevant laws and regulations. (see Appendix II for additional detail.)

Data Management Policies

1. IITS is responsible for leading the collaborative process of managing, securing, and improving our data systems. Leadership areas include:

   a. Researching, acquiring and launching institutional data systems, including initial application training and subsequent upgrades
   b. Managing the risk associated with maintaining data
      1. Developing and periodically reviewing reliable access and security controls (both technological and human) for centrally stored information, and advising data stewards on appropriate protocol for data stored in auxiliary systems.
      2. Informing and periodically reminding all those accessing institutional data of the College's Statement on Confidentiality (to be published).
      3. Securely maintaining centralized College records as well as those stored on network servers, and consulting with relevant data stewards and the College Archivist/Records Manager in adhering to College record retention policies.
   c. Establishing, in consultation with user groups, the systems of record and related protocols to ensure that all data-users are accessing the most accurate, up-to-date data from those systems of record; IITS responsibility includes coordination of the critical data update protocols that involve multiple departments.
   d. Facilitating employee technology training, by establishing and supporting the activities of Application User Groups (either within departments or across divisions)

2. Data stewards are responsible for ensuring the accuracy and reliability of the data within their purview.

   a. Individual offices are responsible for adhering to and periodically reviewing College policies on confidentiality
   b. Individual offices are responsible for updating the system of record (or alerting the data steward for that system of record) of any updated information they receive
   c. Individual offices are responsible for providing appropriate/necessary intra- institutional access to systems of record, with the assistance of IITS
   d. Individual offices are responsible for engaging <u>all</u> departmental data professionals to improve data quality and processes
   e. Individual offices are responsible for function-specific training, cross-training of staff, and documentation of local data management applications.
   f. Individual offices are responsible for securely maintaining records and consulting with the College Archivist/Records Manager in adhering to College record retention policies

3. Application User Groups (either within departments or across divisions) support post-implementation application education and cross-training.

   a. On-going user support/troubleshooting
   b. Demonstration and sharing of techniques for accessing data within legacy, auxiliary, and new data systems

Appendix I – Data Stewards and Sources

A. Data Stewards are individuals who, by virtue of their role at the college and access to specific data, are expected to manage (or steward) the accuracy, completeness, and access to the data under their stewardship. Data stewards are expected to collaborate with producers and consumers of this data to achieve this goal.

B. Data Steward areas and associated data stores and systems

1. Admission: SLATE, PowerFaids, and Admin (Financial Aid)
2. Athletics: Admin, Access to RE and Slate
3. Business Office: Kuali Financials
4. Career Development Office: Raiser's Edge
5. CPGC: Filemaker and Grants tracking within Kuali
6. Dean's Office: Admin, PeopleSoft (effective 7/2013)
7. HAHC: Excel
8. Human Resources: Admin, PeopleSoft (effective 7/2014)
9. Institutional Advancement: Raiser's Edge (RE)
10. Institutional Research: Excel, SPSS
11. Library: Tripod & institutional repository (e-records; e-archives)
12. Registrar: Admin, PeopleSoft (effective 7/2013)
13. Provost's Office: Excel, Filemaker
14. Student Housing Office: Filemaker
15. Study Abroad: admin, Peoplesoft (effective 7/2013)
16. IITS: Admin

C. "System(s) of Record" by Constituent:

1. Applicants: SLATE (Admission Office)
2. Students: Admin, PeopleSoft (effective July 2013)
3. Alumni: Raiser's Edge
4. Parent (after student matriculation): Raiser's Edge
5. Faculty: Admin, Filemaker, Raiser's Edge, Peoplesoft (effective July 2014)
6. Staff: Admin , Raiser's Edge, Peoplesoft (effective July 2014)
7. Vendors: Kuali

Appendix II – Relevant Laws/Regulations/Best Practices

A. Privacy

1. **FERPA** (Family Educational Rights and Privacy Act) protects the privacy of student education records.
   http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

2. **HIPAA** (Health Insurance Portability and Accountability Act of 1996)– HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.
   http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

3. **PCI (Payment Card Industry)--**The Payment Card Industry Security Standards Council web page is a valuable resource regarding the handling of cardholder information:

   https://www.pcisecuritystandards.org/security_standards/index.php
   "The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents."

4. **PII (Personally Identifiable Information)**-- An excellent overview that provides details on protecting personally identifiable information can be found at:

   http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

   This "Guide to Protecting the Confidentiality of Personally Identifiable Information," was written by staff at the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) and focuses specifically on protecting PII information stored on computers. Examples of PII include but are not limited to: Name, such as full name, maiden name, mother�much maiden name, or alias. Personal identification number, such as social security number (SSN), passport number, driver�much license number, taxpayer identification number, or financial account or credit card number; Address information, such as street address or email address. Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

   Organizations are asked to minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

B. Security

1. Identify Theft (Federal Trade Commission). The FTC Red Flags Rule requires many organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations. **www.ftc.gov/redflagsrule**

2. Prevention and detection of Terrorism (U.S. Department of Justice). The Patriot Act authorizes the use of surveillance mechanisms and information-sharing to prevent terrorism . **http://www.justice.gov/archive/ll/highlights.htm**

3. Electronic surveillance (Federal Communication Commission). CALEA (Communications Assistance for Law Enforcement Act) enhances the ability of law enforcement and intelligence agencies to conduct electronic surveillance. **http://transition.fcc.gov/pshs/services/calea/**

4. Tracking of foreign students . The Student and Exchange Visitor Information System (**SEVIS**) is the web-accessible database for monitoring information about exchange visitors, international students and scholars subject to this program. It was established by the Department of Homeland Security, and is administered by the Student and Exchange Visitor Program (SEVP).

Article on the overlap of privacy and security:

http://www.educause.edu/ero/article/civil-privacy-and-national-security-legislation-three-dimensional-view

C. Reporting

1. Sarbanes-Oxley Act of 2002

The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board" to oversee the activities of the auditing profession.

http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:%20

D. Human Subject Research Regulations

1. Haverford College Institutional Review Board Policy: **http://www.haverford.edu/provost/committees/irb.php**

2. U. S. Department of Health and Human Services: **http://www.hhs.gov/ohrp/index.html**