Role and Responsibilities of Princeton University Data Stewards

This document establishes the role and responsibilities of Princeton University Data Stewards to implement process by which University users abide by the Information Security Policy*, Records Management Principles and all other relevant policies.**

Data Stewards, typically Academic Officers and Officers of the Corporation, are the individuals at Princeton who are accountable for providing university-level knowledge and understanding for a specific data area (e.g., student data, financial data, HR data, or alumni and donor data) and for promoting appropriate use and protection of data (electronic and hard copy) through planning, policy, processes, communication, and associated procedures. **Data Stewards may designate an appropriate member or members of their organization to be responsible for the actual implementation and management of the following data-related activities:**

- Operational Oversight
- Data Quality
- Privacy, Security, and Risk Management
- Access and Authorization

- **Operational Oversight**

Data Stewards play a key role in overseeing the life cycle of a particular set of institutional data. Specifically, Data Stewards are responsible for defining and implementing policies and procedures for the day-to-day operational and administrative management of systems and data, including the intake, storage, processing, and transmittal of data to internal and external systems, vendors and other third-parties. To ensure compliance with data policies and procedures, Data Stewards provide training and documentation for individuals/groups who have access to data. As part of the oversight for institutional and departmental data, the Data Steward must document and communicate the classification level for all data in their area and provide guidance on the appropriate use of the data they steward. An example would be establishing guidelines for report writing.

Often, operational oversight may involve multiple Data Stewards. In this case, a high degree of coordination is required to ensure that the processes are aligned among Data Stewards.

Finally, as new data collections are developed and implemented, a Data Steward must be identified and assigned the appropriate responsibilities.

- **Data Quality**

Data Stewards are ultimately responsible for data quality, including the metadata that defines the values, ranges, and parameters acceptable for each data element. Data Stewards work to establish procedures for detection and correction of data quality issues and collaborate with process owners to establish policies, procedures, and internal controls affecting the quality of data. In addition, Data Stewards engage in the ongoing and detailed evaluation of data quality, the identification of anomalies and discrepancies, and to contribute expertise to implement corrective measures.

- **Privacy, Security, and Risk Management**

  In partnership with the Office of Information Technology, Office of General Counsel, and Risk Management, Data Stewards are responsible for security, privacy, and risk management of their data. Data Stewards must establish guidelines and protocols to manage data, ensuring that appropriate controls are enforced in systems and processes. Data Stewards must manage the transfer, retention, archiving, and disposal of data in compliance with institutional policy and regulations. Data Stewards evaluate and respond to suspected or actual data breaches or vulnerabilities. Data Stewards are also responsible for ensuring that the use, sharing, transmitting and destruction of data is appropriately defined, reviewed and approved in University contracts with external vendors that include the data for which they are responsible.

- **Access & Authorization**

  Data Stewards define procedures for access to data, including documenting the criteria for authorization based on role and/or the individual. Responsibilities include oversight of the access request, appropriate training that may be required prior to use of the data, approval, provisioning, regular re-certification of access, and de-provisioning processes.

Data Stewards or their designees have membership in the following:

Data Governance Steering Committee

The Data Governance Steering Committee is an Executive-level group that provides a structure for campus-wide discussions, determining directions and setting strategies concerning the protection of Princeton data and for guiding campus initiatives that relate to the use of University information. Membership is comprised of Academic Officers and Officers of the Corporation from the Office of Finance and Treasury, Office of the Registrar, Office of the General Counsel, Office of the Dean of the Faculty, Audit and Compliance, Human Resources, Office of the Executive Vice President and Office of Information Technology.

Data Management Advisory Group (DMAG)

The Data Management Advisory Group (DMAG), whose membership consists of designees of the Data Stewards, focuses on issues of data management as they relate to student, employee, faculty, financial, facilities, donor and health record data. The group assesses best practices and issues relating to data classification, data sharing, data safeguarding and proper use. The group functions both as a forum to discuss data-related topics that are initiated by the Data Governance Steering Committee and to investigate and recommend best practices and/or policies that require the consideration and possible approval of that Committee.

* Information Security Policy (http://www.princeton.edu/oit/it-policies/it-security-policy/)

**Records Management Principles (https://records.princeton.edu/policies-procedures)