VI-23.00(A) UNIVERSITY OF MARYLAND POLICY ON DATA MANAGEMENT STRUCTURE AND PROCEDURES

(APPROVED BY THE PRESIDENT February 7, 2003; Technical Amendments November 7, 2013)

I. Purpose

The University of Maryland, College Park (UM) recognizes Institutional Data as an asset of the University and has implemented a data management structure that defines five levels of responsibility for Institutional Data within the University.

II. Data Management Structure

The UM data management structure is defined by five levels within the institution and their corresponding responsibilities. The levels and their responsibilities are:

A. Data Owner. The University itself. UM is the owner of all Institutional Data.

B. Data Trustee. Individual UM Vice Presidents. Data Trustees have overall responsibility for the collection of data subsets within their division.

C. Data Steward: Designated senior University officials. A list of current Data Stewards is maintained by the IT Security & Policy Office within the Division of Information Technology (ITSPO). Data Stewards have overall responsibility for subsets of Institutional Data that are managed by their reporting units. Some data subsets may have more than one Data Steward where more than one functional unit uses and collects the same information; e.g., University ID number. With respect to their pertinent subsets of Institutional Data, Data Stewards have specific responsibility to:

1. Understand and implement applicable statutes, regulations, policies and guidelines of the State of Maryland and University of System of Maryland;

2. Adhere to data standards developed by the Division of IT on such matters as data element naming conventions and standard abbreviations, and take steps to assure the integrity, accuracy and completeness of data.

3. Identify the level and type of access accorded to each element of data within data subsets; e.g., public access, UM access, limited UM access, and comply with University Guidelines and Procedures Governing the Inspection of Public Records, VI-5.00(A).

4. Establish protocols, consistent with UM policy, which facilitate appropriate, lawful access to data elements and data subsets.

5. Recommend policies and establish procedures and guidelines to protect and maintain the accuracy and integrity of data subsets.

6. Implement and maintain appropriate security over data.

7. Actively participate to resolve issues that emerge when more than one Data Steward claims responsibility for the same data elements. Disputes will be resolved by the Data Policy Advisory Committee.

D. Data Manager. UM officials and members of their staff who have responsibility to collect, maintain, disseminate, and manage a specific subset of data in their functional area. ITSPO maintains a list of current Data Managers. With respect to those data subsets for which they have responsibility in their functional area, Data Managers have specific responsibility to:

1. Review and act on requests by UM users and members of the public to access data subsets, in accordance with UM policy and protocols;

2. Implement and assure compliance with data access security standards through staff training;

3. Define data elements within a data subset in coordination with the University Data Administrator.

4. Train and assist in data interpretation.

E. Data User: Any UM employee or student who has lawful and appropriate access to a specific subset of data. All users must adhere to federal, State and UM laws, regulations and policies regarding access and maintain the privacy and security of data.

III. Data Security

The Division of Information Technology will:

A. Develop and enforce security procedures and operating practices which support the tenets outlined in this policy. These measures must not interfere with valid use of data for the effective management of the University.

B. Establish procedures which enforce security between applications, i.e., which ensure that access to one application does not afford unauthorized access to other applications.

C. Establish measures to counteract events which compromise data integrity such as system failure, inadvertent manipulation, unauthorized penetration, or unforeseen disasters. These measures include maintaining a proper operating

environment, exercising preventative maintenance checks of safety and early warning sensors, performing sufficient system wide back-ups to enable restoration of operating capability in the event of system outage, and utilizing off-site storage locations for system wide and application back-ups.

D. Provide prudent physical and environmental measures for the hardware, software, and data within its purview.

E. Establish procedures which enforce separation of duties such that personnel who develop or install software cannot alter data or programs currently used for production purposes.

F. Establish procedures such that changes to applications and systems software are controlled according to a formal process, which includes thorough testing in a development environment and movement into a production environment through a defined turnover process.

G. Monitor and review implementation of the defined access rules, to include review of audit reports when available.

H. Ensure security measures are cost-effective and are supported by a risk analysis process. This process compares potential threats to data with the specific vulnerabilities of the IT operation to those threats.

I. ITSPO will maintain a mechanism to facilitate the processes for requesting access to institutional data.

These requirements also apply to any other University entity possessing institutional data.