INFORMATION TECHNOLOGY DATA MANAGEMENT PROCEDURES AND GOVERNANCE STRUCTURE

BALL STATE UNIVERSITY OFFICE OF INFORMATION SECURITY SERVICES

1. INTRODUCTION

If you are responsible for maintaining or using University information in your department, this guide will help you understand who and where to contact for help as well as how university data is management is organized.

2. ROLES AND RESPONSIBILITIES FOR UNIVERSITY DATA MANAGEMENT

"University data" refers to collections of data elements relevant to the operations and management of Ball State University as well as data presented in official reports. The responsibilities and roles for Data Management at Ball State are defined by the following groups:

a. Executive Sponsors: The University Vice Presidents collectively oversee all units and areas within the University; they provide final approval for all data polices.

b. The Data Management Committee: The committee supports environments which reduce the total number of systems, reduce complexity, simplify integration, support data integrity, maintain adequate controls, and improve services to students.

   The committee works to ensure consistent data usage across all university units, helps prevent data misuse and ensure against loss, and strives to deliver greater reporting accuracy so university decision-makers have the most relevant, timely, and high-quality data available. Operationally the committee maintains the university data dictionary, drafts reporting standards, sets census dates, develops schedules for standard reports, determines external reporting responsibilities, and creates and delivers relevant training materials.

   The committee is led by a Chair who coordinates committee meetings and helps ensure participation from data stewards, data reporters, and key information users. Initial members of the Data Management Committee include:

   - Executive Director of Institutional Effectiveness, Chair
   - Assistant Director of University Budgets
   - Associate Dean of University College and Director of Academic Systems
   - Associate Dean, Graduate School
   - Associate Provost and Dean, University College
   - Associate Vice President for Business Affairs and Assistant Treasurer
   - Associate Vice President for Student Affairs
   - Associate VP for Student Affairs and Director of Housing and Residence Life
   - Coordinator of Enterprise Data Analytics and Distribution
   - Director of Advancement Services
   - Director of Facilities Business Services and Transportation Facilities Management
   - Director of Financial Information Systems and Technology
   - Director of Human Resources
   - Director of Office of Information Security Services
   - Director of Information Systems Services
   - Director of Payroll and Employee Benefits
   - Director of Research and Academic Effectiveness

- ➢ Director of Scholarships and Financial Aid
- ➢ Director of Systems Technology, Enrollment, Marketing, and Communications
- ➢ Director, Sponsored Programs Office
- ➢ Registrar and Director of Registration and Academic Progress
- ➢ University Controller

Membership in the Data Management Committee may be altered as recommended by the Data Management Committee and approved by the Executive Sponsors.

c. Data Stewards: The Data Stewards have direct operational responsibly for data within their respective areas including establishing guidelines and profiles for information access, and making recommendations and decisions about individual requests for access. The Data Stewards also ensure against data loss and provide appropriate documentation and training to support Data Reporters and Information Users described below. Members of the Data Stewards are listed in the University Data Stewards form.

For the most up-to-date listing including names and contact information, see the Office of Information Security Services web site at http://www.bsu.edu/security/.

d. Data Reporters: Data reporters are various employees across Ball State University whose job responsibilities require them to access, manipulate, and analyze University data in order to provide information for decision-makers. Data reporters may work within one data system or its components (e.g., financial aid), or they may work across multiple data areas. It is critical that data reporters understand and adhere to data definitions, standards, and practices developed by the Data Stewards and the Data Management Committee in order that reported information is accurate, consistent, timely, and actionable.

e. Information Users: Information users are personnel throughout the University whose job responsibilities require them to make decisions based upon information. Examples of information users include, but are not limited to, the President, vice presidents, deans, directors, department chairs, faculty members, and members of University committees. Information users rely upon data reporters to access, manipulate, and analyze University data in order to provide information that is accurate, consistent, timely, and actionable.

3. User Support

If you need assistance with data or reporting, contact the appropriate area as identified below:

a. Data stewards will provide user support, primarily through documentation but also, as needed to assist data users in the interpretation and use of institutional data. This responsibility may be delegated to the data managers. The list of data stewards and their roles and contact information is available on the Office of Information Security Services web site at http://www.bsu.edu/security or on the Information Technology policy web site at http://www.bsu.edu/security/itpolicy.

b. The data reporters and information users will be responsible for their appropriate use and consistent interpretation of the data which they access.

c. All users should bring data problems and suggestions for improvements to the attention of the appropriate data stewards or the Data Management Committee.

If you do not know the area to contact, you may contact the Technology Helpdesk at 765-285-1517.

4. Handling Confidential Information

Mishandling of confidential information is extremely serious and may result in civil or criminal penalties as well as termination from employment. *Review this guide and the related procedures below carefully before working with* *university confidential information.* The following laws and regulations governing the security and privacy of confidential records are among the most important and frequently relevant to University operations:

a. Student Information: The *Family Educational Rights and Privacy Act* ("FERPA") is a federal law protecting student education records. It can be found at http://www.ed.gov/ferpa/.

b. Health Care Information: The *Health Insurance Information Portability and Accountability Act* ("HIPAA") is a federal law regarding privacy of certain healthcare information. It can be found at: http://www.hhs.gov/ocr/hipaa/.

c. Social Security Numbers: The Indiana *Release of Social Security Number* law can be found at Indiana Code at IC 4-1-10 at http://www.in.gov/legislative/ic/code/title4/ar1/ch10.html.

d. Motor Vehicle Records: The Indiana law regarding *Disclosure of Personal Information Contained in Motor Vehicle Records* can be found in the Indiana Code at IC 9-14-3.5 at http://www.in.gov/legislative/ic/code/title9/ar14/ch3.5.html.

e. Financial Records: The Red Flags Rule was created by the Federal Trade Commission (FTC) to help prevent identity theft, it can be found at http://www.ftc.gov/redflagsrule/.

In addition to the laws and regulations described above, Ball State University has established certain procedures and practices related to confidential information:

f. Information Security: University policy regarding information security practices, mobile access, servers, hosted systems, data extraction, general security requirements, and official procedures for reporting a suspected information security breach or incident can be found at http://www.bsu.edu/security/itpolicy.
It is important to become familiar with these policies and procedures before attempting or requesting access to University data.

g. Research: The Office of Research Integrity has created procedure and standards regarding research use of human subjects, animal care and use, biosafety, and radiation safety. More information is available at http://www.bsu.edu/researchintegrity/.

Other state and federal laws, administrative agency rules, and contractual or association requirements may apply to your specific situation and you should check with your supervisor.

5. Who May Have Access To University Data

The data stewards will have primary responsibility for granting access to confidential university data. The following procedure apply when accessing university data:

a. Read-Only Access: View or read-only access to administrative data will be provided to employees to support university business and for performing official job duties. However, access and use of data may only be completed as required for the performance of assigned job functions, and not for personal use or other purposes unrelated to official duties and responsibilities. Access does not imply a right to view or use data for any purpose other than official job duties. The data steward has primary responsibility for proper use of institutional data; individual data users will be held accountable for their accesses and uses of the data.

b. Update Access: Change, or update authority shall be granted only to personnel whose job duties specify and require responsibility for data update. The data steward is responsible for setting policies regarding the manipulation, modification, or reporting of institutional data elements and for creating derived elements, which are also institutional data.

c. Release of Student Data: Only student data elements designated as "directory information" (as defined by FERPA) can be *externally disseminated* for official or "nonofficial" reporting. Even release of directory information must be carefully considered. Release of all other student data must be approved by the responsible data steward.

d. Social Security Numbers: Access to Social Security Numbers is strictly constrained to legal necessary. Inappropriate use or storage of Social Security Numbers may lead to unauthorized disclosure which carries potential criminal and civil penalties. All use, including read-only access requires explicit authorization for each business case from the Data Standards Committee and the Office of Information Security Services.

6. How University Data Is Categorized, How It May Be Used, and Who May Access It

Data will be classified by the Data Stewards according the categories and the following general usage guidelines, and decision making process described below.

a. Classification of Data: Data will be classified into one of four broad classifications:
   i. Critical data: Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, in the event of unauthorized access to this type of information.
   ii. Limited-access data: Legal, ethical, or other constraints prevent use without specific authorization; selective access may be granted.
   iii. University-internal data: These data may be used by all eligible employees of the University, without restriction, in the conduct of University business. Non-business-appropriate use of the data is prohibited.
   iv. Public data: There are few restrictions; general public may be granted access. Some data elements classified as public may have certain dissemination restrictions.

b. Use of University Data Generally: Unless designated otherwise, all institutional data will be treated as University-internal data. Data Stewards are responsible for identifying and classifying data into Limited- Access or Critical as required by policy, legal, ethical, or externally-imposed constraints. The Data Stewards will work together to define a single set of procedures for requesting permission to access limited-access institutional data elements, and will be jointly responsible for documenting these common data access request procedures. Each data steward will be individually responsible for documenting data access procedures that are unique to a specific information resource or set of data elements.

c. Decisions About Data Access: Data stewards establish standard rules, guidelines, and profiles for data access, and decide about individual requests to access data within the guidelines established by the Data Management Committee. When necessary, the Data Management Committee will make the final determination on data restrictions and requested access rights to institutional data. The Office of Information Security Services will then implement the final decision regarding data access.

d. Critical and Limited Access Data: All data users having access to critical or limited-access institutional data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of the data they access.

e. Reporting Data Errors: The data steward or delegated data manager is responsible for data integrity, responding to questions about the accuracy of data, and correcting inconsistencies if necessary. Upon notification of erroneous data, corrective measures must be taken as soon as possible to correct the cause of the erroneous data, correct the data in the official storage location, and notify users who have received or accessed erroneous data.

7. Where Data May Be Stored

Data stewards will work with Information Technology to ensure compatibility, accessibility, and congruent interfaces among institutional systems and data elements and will make recommendations regarding the purchase or continued operation of systems based on these principles:

a. Storing Social Security Numbers Outside of Central Systems: Social Security Numbers may not be collected from individuals nor stored on departmental servers; exceptions will only be made in extreme circumstances and must be approved by the Office of Information Security Services, the Data Stewards, and the Data Standards Committee with notification to the Executive Committee.

b. Storing Other Critical and Limited Access University Data: All systems which store, transmit, or process critical and limited-access university data require special security considerations. Contact the Data Standards Committee or the Office of Information Security Services for security requirements, more information can be found here http://www.bsu.edu/security/.

c. Storing Public and University-Internal Data: Departments are expected to identify appropriate server locations for storage of data extracted from central sources or derived through department operations. Contact the Office of Information Security Services for general security requirements.

d. Storing Student Directory Information: A student may choose to restrict access to any directory information at any time. All systems which make student directory information available to unrestricted audiences must be updated daily to reflect student's directives regarding release of directory information.

e. Evaluation and Assessment Data: All program evaluation and assessment data must be stored in such a way that responses are not associated with individual names or Social Security Numbers. Linkage files containing the association of protected data to individuals must be placed in different directories and with different naming conventions to obscure the connection, and must be permanently deleted when no longer needed.

f. Data Backup and Recovery: The data steward is ultimately responsible for defining and implementing policies and procedures to assure that data are backed up and recoverable in response to events that compromise data integrity.

g. System-of-Record and Data Retention: The data steward will determine the official data storage location (or system-of-record) for each data element. The data steward will also determine archiving requirements and strategies for storing and preserving historical data for each data element. Generally, Banner and the related ERP systems provide the system of record for most University data. Other systems such as those run for departmental purposes will generally not be directly connected with reporting systems such as Argos.

8. Data Documentation

The data steward is responsible for ensuring complete and accurate data documentation and that it is appropriately maintained and shared with relevant units. Documentation must include algorithms or decision rules for the derivation of data where appropriate, and data views must indicate the reference to the data elements which comprise the view and description of the rules by which the view is constructed. Data stewards will also provide overview documentation for databases, data structures, and update-cycles necessary for the accurate interpretation of the data as appropriate.

The Data Management Committee will receive documentation from the data stewards in electronic format and use this information for maintaining the University Data Dictionary and making it readily accessible to all interested parties. Proposed changes in data definition characteristics will be noted to the Data Management Committee and recorded in the University Data Dictionary in advance of the change.

9. Acknowledgement

Substantial portions of this policy are based upon similar documents from Indiana University and the University of Nevada at Las Vegas and are used with the permission of those institution