Policy Archived. Please refer to the University Policy Library for current version.

830 Data Security and Management

Last updated on: December 14, 2018

Authority: Approved by the Board of Trustees

830.1 Institutional Data and Obligations

Institutional data are a valuable resource to Indiana State University. The environment for data security is complex and constantly changing. A variety of federal, state, and industry regulations establish both personal and institutional responsibility for data security. In addition to these, ethical and professional considerations create an obligation for all members of the ISU community to care for institutional data with the highest levels of awareness and best practices.

830.1.1 Scope. Data are considered to be University resources and as such, policies controlling the creation, receipt, transmission, processing, use, storage, printing, or dissemination of data are set by the University. These policies will be augmented as needed by specific standards and procedures that will apply at the institutional level. Nothing in this policy shall negate the provisions of the Policy Library Policy 370 Intellectual Property.

830.1.2 Definition of Institutional Data. Indiana State University institutional data are data that are:

- Created, received, processed, transmitted, or stored as a result of educational, clinical, research, patient-care, or service activities; or
- Substantive, reliable, and relevant to the planning, managing, operating, documenting, staffing, or auditing of one or more major administrative functions of the University; or
- Used to derive any data element that fits the above criteria.

This definition applies regardless of the form or medium on which the data are created, received, processed, transmitted, or stored.

830.2 Types of Data

In order to communicate clearly about data management practices, it is necessary to recognize that there are different categories and classifications of institutional data

830.2.1 Categories of Data. Data categories are defined based on the function and/or use of institutional data. General institutional data categories include:

- Alumni data
- Contracts and grants data
- Research data
- Employee and benefits data
- Facilities data
- Faculty data
- Financial and budget data
- Health data
- International programs data
- Library data
- Purchasing and travel data
- Student and applicant data
- Instruction-related data

830.2.2 Classifications of Data. Data classifications are defined based on the need to ensure the security and privacy of institutional data. Data classifications are:

830.2.2.1 Public Data. Information and data that are intended for public view.

830.2.2.2 University-Internal Data. Data used internally to University operations or with selected University appointees or partners for ISU business purposes. Access to University Internal Data should be determined based on the job responsibilities of the employee, appointee, or partner.

830.2.2.3 Restricted Data. Data that are sensitive or confidential and, as a result, require specific authorization for access.

830.2.2.4. Highly-Restricted Data. Highly confidential data that, if released, could result in criminal or civil penalties, identity theft, personal financial loss, or invasion of privacy.

830.3 Access to and Handling of Data

All ISU employees are responsible for handling institutional data properly based on its classification. Data handling includes all activities associated with the creation, storage, transmission, printing, backup, retention, disposal and publication of ISU data.

830.3.1 Control of Data Access.

830.3.1.1 Access. Access to data other than public data shall be accomplished through the use of usernames (ID) and passwords. Elements used to control access to data (like IDs and passwords) are not to be shared with other employees. As noted above, data dissemination is driven by 1) the classification of the data, and 2) the need to know.

830.3.1.2 Supervision of Students. Students who access ISU data other than public data will be supervised by full-time ISU personnel; student and student employee access to data other than public data shall be the responsibility of the full-time employee responsible for supervision of the student or student employee. Students and student employees are required to complete appropriate training in order to have access to non-public University Data.

830.3.2 Data Handling and Use. Users of institutional data must:

- Access data only related to their conduct of University business, and in ways consistent with furthering the University's mission of education, research, and public service
- Respect the confidentiality and privacy of individuals whose records they may access
- Observe any ethical or legal restrictions that apply to the data to which they have access
- Abide by applicable laws, regulations, standards, and policies with respect to access, use, disclosure, retention, and/or disposal of information

Users of institutional data must not:

- Disclose data to others except as required by their job responsibilities
- Use data for their own or others' personal gain or profit, except as set forth in the Policy Library Policy 370 Intellectual Property.
- Access data to satisfy personal curiosity.

University procedures for data handling are provided in the Indiana State University Data Storage Policy Matrix, documented as part of Office of Information Technology standards.

830.4 Export Control for University Data

Indiana State University and its faculty, staff, and students must comply with all United States export control laws and regulations. Export control laws cover data as well as equipment and other assets. Faculty, staff, and students are responsible for understanding whether data they are working with are covered by export regulations, when there is a need to share data with or expose data to individuals outside the United States. The Office of the Provost can advise on the requirements for specific data.

830.5 Data Security Incidents

830.5.1 Definition of a Data Security Incident. A data security incident is an occurrence, threat, or possible compromise involving institutional data that are not Public Data. Such a threat may be associated with a hardware component (e.g. a laptop, a smartphone) or an account. Quite often, such incidents occur when a virus or malware infects an institutional computer, and the data on or accessible to that device or the accounts that are used on that device are subject to compromise as a result. In other cases, an action taken by an employee or student, such as theft, loss, or exposure of printed materials containing institutional data that are not Public Data, may constitute a compromise.

830.5.2 Discovery of a Data Security Incident. Discovery of a possible data security incident may occur in a variety of ways:

- ISU security or other software or network protocols may demonstrate that a possible compromise has occurred
- External security agencies may notify us that a possible compromise has occurred
- A computer user may notice unexpected behavior and request assistance from support resources, who discover that a possible compromise has occurred
- Transactional or procedural activity may reveal that data has been compromised or released.

In some cases, discovery is made by information technology and/or security professionals; in others, discovery may be made by an individual employee and/or that employee's management.

830.5.3 Reporting of a Data Security Incident. In all cases, when a possible data security incident is suspected or identified, institutional employees must report the incident immediately upon discovery. An individual employee should also report to his or her supervisor any incident that appears to relate to a data security breach.

University procedures for reporting data security incidents can be found **HERE**