Institutional Data Classification: Basics

Issued: 06/01/2015
Revised: 06/01/2015

FOUR CLASSIFICATION LEVELS OF INSTITUTIONAL DATA

Institutional data is any and all data used to conduct university business or research. The Institutional Data Policy (IDP) defines four levels of classification: public, internal, private, and restricted. The data classification level is a formal categorization and labeling of data based upon the sensitivity and regulatory privacy requirements for protecting the data.

Public: Public data is intended for public use and has no access or management restrictions.

Internal: Internal data is used to conduct university business and operations by those whose jobs require it, and is the default classification level.

Private: Due to laws or regulations or other requirements, private data may only be accessed with special authorization. Unauthorized access or disclosure may result in administrative or legal action.

Restricted: Due to laws or regulations or other requirements, restricted data may only be accessed with authorization that is strictly limited. Unauthorized access or disclosure may result in substantial administrative or legal action (such as fines). Restricted data must always be encrypted.

Note that personal data -- information not related to university business – is not subject to data classification. Personal data used on university owned devices must adhere to the Responsible Use of University Computing and Network Resources policy.

> *Examples:* Here's how some Family Educational Rights and Privacy Act (FERPA) data is classified. A student's directory information is classified as **public** if not withheld by the student's written request; if withheld per the student's written request, it is classified as **private**. Student educational records are classified as **private**. Student medical treatment records are classified as **restricted**.

For more information about classifications, read the policy and view online training. For more information about the Institutional Data or Responsible Use policies, contact itpolicy@osu.edu.

CLASSIFICATION LEVEL DETERMINES DATA ACCESS & PROTECTION REQUIREMENTS

The classification of institutional data determines who may access the data and how much protection the information requires. Correct classification ensures that the university complies with laws, regulations and university requirements.

The Information Security Control Requirements (ISCR) provides detailed implementation specifications for the security controls defined in Ohio State's Information Security Standard (ISS). The ISCR is also linked to Ohio State's Institutional Data Policy (IDP). The control requirements in the ISCR are specified according to the level of institutional data being protected, as defined by the IDP.

The ISCR associates a security categorization level, or "S-level", with each of the IDP's four classification levels: S1 (Public), S2 (Internal), S3 (Private), and S4 (Restricted).

> *Examples:* IDP data classification levels are shown below in columns in the control requirement matrix of the ISCR, specifying access and protection requirements.

THE OHIO STATE UNIVERSITY — Information Security Control Requirements
Enterprise Security

INSTITUTIONAL DATA RISK

DAT1	**Institutional data-related risk** To ensure the proper classification, labeling, and handling of institutional data. Note: Data may be in digital or physical form.	P1

The following control requirements are implemented as indicated by the data classification level:

	ISS	S1 (Public)	S2 (Internal)	S3 (Private)	S4 (Restricted)
DAT1.1	Data must be categorized according to Ohio State's *Institutional Data Policy*. *(NIST SP 800-53 RA-2)*	DAT1.1.1 Data categorization (see page 74) DAT1.1.2 Critical system list (see page 74) DAT1.1.3 High availability system list (see page 75)	DAT1.1.1 DAT1.1.2	DAT1.1.1 DAT1.1.2	DAT1.1.1 DAT1.1.2
DAT1.2	University records must be managed according to records retention and disposition schedules. *(NIST SP 800-53 SI-12)*	DAT1.2.1 Records management review (see page 76)	DAT1.2.1	DAT1.2.1	DAT1.2.1
DAT1.3	Data must be protected during storage as indicated by the data classification level. *(NIST SP 800-53 SC-28)*			DAT1.3.1 Portable device and storage media encryption (see page 76)	DAT1.3.1 DAT1.3.2 Secure data storage (see page 77)

Information Security Control Requirements Issued: v1.2.1 01/1/2015
Section 6 Control Requirements: DAT1
Page 18

ISCR Example: "Institutional data-related risk", or "DAT1", is one of thirty risk areas defined by the ISS and covered in the ISCR. This is a portion of DAT1's matrix of control requirement specifications according to IDP data classification level.

For more information about the Information Security Standards or Control Requirements, contact riskmgmt@osu.edu.