THE OHIO STATE UNIVERSITY

Institutional Data
Frequently Asked Questions (FAQ)
Office of the Chief Information Officer

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

Frequently Asked Questions (FAQ)

Issued: 09/15/2014
Revised: 05/16/2016

Q. **Contacts:** Who can I contact with comments, questions, and suggestions?

Submit comments, questions, and suggestions to ITPolicy@osu.edu.

Q. **Related Materials:** Where can I acquire the Institutional Data policy and related materials?

- Institutional Data home page. This is the entry point to the 2014 revised policy, with links to other policies. Short URL: https://go.osu.edu/idp.
- Institutional Data policy. This is the actual policy in .pdf format. Short URL: https://go.osu.edu/idp-document.
- Institutional Data Element Classification Assignments. Maps institutional data elements to the appropriate data classification levels. Short URL: http://go.osu.edu/idp-elements.
- Permitted Data Usage By Activity. Identifies which classifications of institutional data are permitted for specific data user activities. Short URL: http://go.osu.edu/idp-activities.
- Permitted Data Usage By Service. Identifies which classifications of institutional data are permitted for specific core or hosted services. Short URL: http://go.osu.edu/idp-services.

Q. **Changes:** What are the substantive changes from the previous (2007) version of the Institutional Data policy?

Substantive changes from the previous (2007) version of the Institutional Data policy's ***Policy*** section include:

- Restructured and simplified policy for enhanced clarity and readability.
- Clarified existing institutional data definition in regard to research data and data formats.
- Added definition for personal data.
- Updated Data Classifications:
  - Changed the name of "Limited Data" to "Internal Data" to better reflect classification description.
  - Added an additional classification of "Private Data" to allow for more flexibility in the application of controls for data access, protection and management.
- Integrated data classifications to the Information Security Standard for data security controls.
- Addressed additional areas of data lifecycle management in regard to institutional data, including records management, release and data disposal.

Substantive changes from the previous (2007) version of the Institutional Data policy's ***Procedures*** section include:

- Introduced reference documents:
  - Institutional Data Element Classification Assignments. Maps institutional data elements to the appropriate data classification levels.
  - Permitted Data Usage By Activity. Identifies which classifications of institutional data are permitted for specific data user activities.
  - Permitted Data Usage By Service. Identifies which classifications of institutional data are permitted for specific core or hosted services.
- Updated data roles and responsibilities:
  - Replaced Data Trustee role with Institutional Data Classification Committee (IDCC).
  - Added Data Manager role to reflect operational and functional management responsibilities at a unit level.
  - Clarified responsibilities of each role (and IDCC) and moved to "Responsibilities" section.
- Clarified institutional data training requirement for Restricted Data classification.
- Articulated steps to take for a suspected data exposure or loss.
- Clarified user and university responsibility for Private Data.
- Updated contacts to add additional university offices pertinent to data classification and management.

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

Q. **Data Classifications:** While talking about the IDP, why do the people in my organization's IT group use terms like "S3 data" and "S4 data"?

The Information Security Control Requirements (ISCR, https://go.osu.edu/infosec-iscr) provides detailed implementation specifications for the security controls defined in Ohio State's Information Security Standard (ISS, https://go.osu.edu/infosec-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 data classification level is a formal categorization and labeling of data based upon the sensitivity and regulatory privacy requirements for protecting the data. Ohio State's IDP defines four levels of data classification. The ISCR associates an "S-level" with each IDP classification level: S1 (Public), S2 (Internal), S3 (Private), and S4 (Restricted).

For more information about data classifications and the Information Security Control Requirements, see "Institutional Data Classification: Basics" (https://go.osu.edu/idp-basics).

For more information about the ISS & ISCR, contact riskmgmt@osu.edu.

Q. **Computer Based Training:** When will the Institutional Data policy training be available on BuckeyeLearn?

In mid-May 2016, the Office of the CIO released a new course *Protecting Institutional Data* on BuckeyeLearn.

Protecting Institutional Data replaces the Carmen-based *Institutional Data Policy Course* and *Institutional Data Policy – Faculty* courses. Both Carmen courses were configured to not accept new self-registrations, although anyone already registered may complete the training before the two courses are completely deactivated in June 2016.

Data users required to complete the training in order to get access to systems, or to meet local unit requirements, should refer to the "Institutional Data Policy Training" knowledge base record (https://go.osu.edu/idp-training) to learn how to self-enroll in the training.

After completing the training, you will be able to:

- Explain your responsibilities for accessing and handling institutional data
- Identify the four classifications of institutional data
- Describe how you are permitted to use each type of institutional data
- Explain what you should do if you suspect the loss, unauthorized access, or exposure of institutional data

The Institutional Data Policy Course includes the Institutional Data Usage and Confidentiality Agreement (https://go.osu.edu/idp-agreement) as part of the final quiz.

Q. **SEC100 - Compliance Training Report:** What is this report and who is authorized to access it?

The Institutional Data Policy Training Report has been available through eReports for many years. Senior Fiscal Officers (SFOs) have been provided access to this report and selected departmental IT representatives may access the report with authorization from their SFO.

Now that IDP training has been moved to BuckeyeLearn, the SEC100 report has a "blind spot" since only Carmen grades are available for it to report. Combined with the planned changes to both Carmen and eReports, BuckeyeLearn will be the authoritative source for IDP training compliance reporting.

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

Q. **Carmen Courses:** I took Carmen-based Institutional Data Policy training. Will I need to also take the IDP training again using BuckeyeLearn?

It depends on when you most-recently completed your Carmen-based IDP training.

- *Completed before May 2015:* The training offered via Carmen prior to 04/30/2015 was based on the "old" IDP classification model (Public, Limited & Restricted). There are no plans to carry forward grades for the "old" IDP courses to BuckeyeLearn.

  Institutional data users who completed Carmen-based training before 04/30/2015 will need to complete the BuckeyeLearn course to remain compliant with the IDP.

- *Completed since May 2015:* The training offered via Carmen since 04/30/2015 was based on the "new" IDP classification model (Public, Internal, Private & Restricted). Grades for the "new" IDP courses will be carried forward to BuckeyeLearn.

  Institutional data users who completed Carmen-based training since 04/30/2015 will be considered compliant with the IDP.

Q. **IDP Training Requirements:** Who is required to take IDP training?

All institutional data users are encouraged to complete IDP training, which typically takes less than an hour.

Here's an index of several sites (but not all) that describe who needs to complete IDP training. In addition, some units or work groups may require all members to complete IDP training independently of the requirements cited below. Please contact ITPolicy@osu.edu if you are unsure if you are required to complete IDP training.

- In the "Responsibilities" section, the IDP document indicates all institutional data users must "Complete the Institutional Data Policy course if restricted data is accessed."

  While IDP training is not required if restricted data is not accessed, the IDP indicates institutional data users "1. Understand and comply with university policies and standards for the access, use, disclosure, and protection of institutional data, including the Ohio State Information Security Standard." IDP training is one way for institutional data users to accomplish this.

  See https://go.osu.edu/idp-document

- In "Step 4" of Security Workflow and Roles, system users must "Complete Institutional Data Policy online training prior to being granted access to any of the Administrative Systems" which (as of May 2016) "include: PeopleSoft, eReports, BuckIQ, Operational Data Stores, Financial Data Warehouse, Human Resources Data Warehouse, Student Analytics, and BuckeyeOasis (university eApplications)."

  See https://ocio.osu.edu/service-details/administrative-systems/general-information/security-workflow-and-roles

- In "IT16.1.2", the Information Security Control Requirements (ISCR) indicates "Organizations must ensure that all users of S4 (restricted) institutional data participate in university-approved institutional data awareness training. Users of S4 (restricted) institutional data must participate in training before they are granted access to S4 (restricted) institutional data. Additionally, users must participate in any regulation-specific awareness training before they are granted access to regulated data. Users must participate in one institutional data awareness training annually."

  Please note the ISCR includes an annual training requirement for those who work with restricted data.

  See https://go.osu.edu/infosec-iscr

Applies to: Faculty, staff, students, contractors, volunteers, visitors, sponsored guests of academic and administrative units, and affiliated entities who have access to institutional data.

- In "Special Considerations" of the eSignature Service Catalog entry, IDP consideration are cited including required IDP training for those with Author and Sender roles.

  See https://osuitsm.service-now.com/selfservice/view_service.do?service=Esignature

Q. **IT16 Requirements:** I reviewed the requirements for "IT16 User-related risk" in the Information Security Control Requirements (ISCR, https://go.osu.edu/iinfosec-iscr). Does the time I spend completing IDP training count towards my annual security awareness activities?

IDP training does not contribute to one's security awareness activities. Always consider IDP training requirements separately. For example, the ISCR's "IT16 User-related risk" is only one of several instances where IDP training is a requirement.

Q. **Contacts:** Who can I contact with comments, questions, and suggestions?

Submit comments, questions, and suggestions to ITPolicy@osu.edu.