This is an interim policy.

Disclosing Institutional Information to Third Parties

DM-02 - Interim

About This Policy

Effective Date:
10-16-2014

Last Updated:
07-01-2014

Responsible University Office:
Committee of Data Stewards

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office
uipo@iu.edu

Back to top

Scope

All agents of the university who have a need to disclose institutional information classified as public, university-internal, limited access/restricted, or critical to a third party.

Back to top

Policy Statement

All authorized agents of the university who have a business need to disclose university institutional information to a third party must be aware of and take proactive steps to reduce the risks associated with the sharing of that information.

Back to top

Reason For Policy

The university has a responsibility to exercise prudent stewardship over the information with which it has been entrusted, and certain information is subject to additional legal and contractual requirements.
The university also recognizes the need to share institutional information with partners to accomplish its mission and that, when disclosing this information, the university must exercise due care. Furthermore, to ensure compliance with applicable federal and state laws, regulations, and university policies, it is vital to evaluate and approve the ability of third parties to appropriately handle and protect information before information is shared.
This policy will assist the university in managing the risks inherent in the disclosing of institutional information.

Back to top

Procedure

Prior to disclosing institutional information, the agent is responsible for initiating and managing the process below to ensure that:

- there is an adequate understanding of the third party's security environment;
- business needs, risks, and mitigating safeguards are analyzed and documented; and
- institutional information is adequately protected.

1. If the information to be shared is classified as public, the agent must:
    1. For situations involving the provision of goods and services, seek advice from the appropriate Data Steward(s) and the Purchasing Department on relevant procedures.
    2. If the request is made pursuant to the Indiana open records statute, seek advice from the Office of the VP and General Counsel.
2. If the information to be shared is classified as university-internal or limited access/restricted, the agent must:
    1. Seek advice from the appropriate Data Steward(s) and, as appropriate, Legal Counsel: there may be a need for an agreement, memo of understanding, or other documentation in disclosing information with third parties.
    2. For situations involving the provision of goods and services, consult with the Purchasing Department to assure that an appropriate agreement (i.e. contract, memo of understanding, etc.) with the third party is in place and that it contains the appropriate data security protection language.
3. If the information to be shared is classified as critical, the agent must:
    1. Initiate a data security review of the third party's ability to appropriately handle and protect the shared information by [link to description of process]. The data security review will include:
        1. completion of a data security questionnaire [provide link],
        2. review by the University Information Security Office (UISO), and other parties as deemed appropriate by the Data Stewards and
        3. approval by the Data Steward responsible for the institutional information involved.
    2. Seek advice from the appropriate Data Steward(s) and, as appropriate, Legal Counsel: there may be a need for an agreement, memo of understanding or other documentation in disclosing information with third parties.
4. It is recognized that in some cases the university is required to share information in compliance with applicable law, and that disclosing may need to occur regardless of the third party's willingness to address risks raised by University's security review, and/or enter into an agreement with the university, and/or due to a compressed timeline. In such situations, the law requiring disclosing, the security concerns raised, and the response of the third party should be documented.

Back to top

Definitions

Disclosing information--Data can be shared with a third party in many ways including:

1. Access of information; examples include gaining entry through either the IU network or internet hosted application that requires authentication; logging into PayPal or OneStart portals, IUIE, SIS/HRMS or other systems to view/obtain/use the data therein;
2. Acquisition of existing data: examples include subscribing to databases containing critical information, receiving information collected by a third party. This type of data will rarely become institutional information for the purposes of this policy;
3. Collection of new data: examples include account creation that requires user information; web forms filled out by students, staff or public; payment transactions; registration for classes or training sessions;
4. Disposal of Information: examples include shredding, incinerating, or otherwise destroying records; secure data deletion; disk and memory wiping.
5. Maintenance of information: examples include warehousing paper or electronic records at a third party site; using a hosted platform provider to store institutional information; email outsourcing;
6. Storage of Information: examples include POS unit for credit card sales, archiving electronic or paper records either on or off-site; saving electronic files to a server either at IU or at a vendor location;
7. Transport (transfer?) of Information; examples include courier service for delivery of sensitive documents or files; electronic file saved to a vendor location; transporting of medical records electronically among health care providers and/or insurers; saving, uploading, downloading or viewing information on a network; POS systems which accept and send credit card data; vending machines which accept and send credit card data to process transactions;
8. Use of information: examples include accessing institutional information to generate queries or reports; using data obtained from magnetic cards used for security systems or for payments; using health information to provide services or process benefits requests; using SSN's and other personally identifiable information to access and print W2 forms.

Agents of the university –An individual authorized to act on behalf of the university and its affiliated organizations. For purposes of this policy, the agent will generally be a faculty or staff member.

Third party -- A separate legal entity that has a business, contractual, legal or other relationship with the university, approved external agencies, and affiliated organizations.

Back to top

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances, involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources for more detail.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Back to top

Additional Contacts

Maintained and revised as necessary by the University Information Policy Office under the direction of approved data management committees.

Office of the Vice President for Information Technology
University Information Policy Office

Back to top

History

Draft policy moved to interim status October 16, 2014.