ADMINISTRATIVE PROCEDURE

Procedure for Reviewing Requests for Access to University Information for Internal Use

Procedure Contents

- **Related Policy**
- **Entities Affected**
- **Procedure Context**
- **Procedure**
- **Forms/Instructions**
- **FAQ**
- **Related Information**
- **History**

Effective Date: 22 October 2012
Last Updated: 22 October 2012
Responsible University Officer:
VP Technology/CIO

Procedure Owner: J. Kelly Flanagan
(responsible for developing, implementing, & managing the procedure)
Procedure Contact: Christine Tolman
(First point of contact for procedure users)

RELATED POLICY: Information Security and Appropriate Use

ENTITIES AFFECTED BY THIS PROCEDURE: Any persons with responsibility for reviewing and approving requests for access to university information

PROCEDURE CONTEXT:

The value of information as an institutional resource is enhanced through appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Therefore, permission to access institutional data should be granted to all authorized employees of the university for all legitimate university purposes.

PROCEDURE:

1. Verify that the request is for a legitimate university purpose (as indicated by line leader's approval).

2. Clarify the request
   a. Is the requested information within your stewardship?
      i. If more than one information steward is a stakeholder, contact an *Information Request Coordinator* for help.
   b. If the requested information is data
      i. Have the specific data fields been identified?
      ii. Has the type of access for each data field been described? (Read Only, Update, Delete, or Create)?
   c. How current does the information need to be?
   d. Are the authorizations for access for a single person or a group?
   e. What is the best way of delivering the information requested (web service, data mart, or data feed)?

   NOTE: Information Request Coordinators in the Office of Information Technology are available to assist in clarifying the information request. They can help identify the specific data fields and the best means (web service, data mart, or data feed) of providing the requested information.

3. Determine whether the requested information is Public, Confidential, or Restricted (see Information Classification table below). Information that has not yet been classified is considered Confidential until a classification is proposed by the Information Steward and approved by the Information Trustee.
4. Given the classification of the information requested, determine the access, usage, security, transmission, and storage requirements using the following table as a guide.

BYU INFORMATION CLASSIFICATION			
	Public	**Confidential**	**Restricted**
Classification Description	Information that is available to the general public with no existing legal or regulatory access restrictions	Non-public sensitive information that must be protected due to proprietary, ethical, or privacy considerations	Non-public sensitive information that must be protected by law or policies
Examples	Course catalog, directory information including addresses (NOTE: Individuals can request that access to their public information be restricted in which case it is treated as Restricted information.)	Full date of birth, ethnicity, donor contact information, contracts	Student Academic Record (FERPA), non-directory information, social security number, credit card number, health insurance policy ID number, driver license number
Access and Usage Restrictions	Available without restrictions for internal use.	Limited to those with a need to know and approved by their line manager and the information steward.	Limited to those with a need to know as permitted by law or regulation and approved by their line manager and the information steward
Training Requirements	None	As needed (e.g. FERPA, PCI)	As needed (e.g. FERPA, PCI)
Security Requirements	None	Verified compliance with **BYU's Basic Security Standards**	Verified compliance with **BYU's Enhanced Security Standards**
Transmission Requirements	None	BYU-approved encryption is strongly recommended when transmitting information through a network. Third party email services are discouraged for transmitting confidential information.	BYU-approved encryption is required when transmitting information through a network. Third party email services are not authorized for transmitting Restricted information. Restricted numbers may be masked instead of encrypted.
Storage Requirements	None	BYU-approved encryption is strongly recommended and secure location. Storage by third party (cloud) services is permitted (see *Cloud Computing Guidelines* for special considerations) See BYU's Basic Security Standards.	BYU-approved encryption is required for some data elements (e.g., credit card numbers). Storage by third party (cloud) services permitted only if a contract approved by the university CIO is in place with the provider. (See *Acquiring Cloud Services* procedure) See BYU's Enhanced Security Standards.

5. Go to www.info.byu.edu to complete the Information Sharing Agreement by adding Terms of Use as suggested by the table above and any unique to your organization.

6. Send the proposed agreement to the Requester for their consideration.

7. If the requester accepts the terms, access is granted and the Information Sharing Agreement is added to the information governance repository for future reference.

FORMS/INSTRUCTIONS

The key online forms related to this procedure are:

- **Access Request Form**
- **Information Sharing Agreement**

FREQUENTLY ASKED QUESTIONS

There are no frequently asked questions for this procedure—yet.

RELATED INFORMATION

- *Access to Student Records Policy*
- *Access to Student Records Procedure*
- *Institutional Assessment and Analysis; Information/Study Request Policy*
- *Computer and Electronic Communications General Use Policy*

HISTORY

Effective:
22 October 2012

Superseded:
XXXXXXX Procedure