ADMINISTRATIVE PROCEDURE

Information Security Program

Responsible University Officer: VP Technology/CIO
Procedure Owner: J. Kelly Flanagan
Procedure Custodian: Todd Brown

Effective Date: April 7, 2017
Last Updated: November 9, 2017

Contents

RELATED POLICY: Information Technology: Information Security and Appropriate Use

APPLICABILITY

This program applies to all university academic and administrative units that store, process, or transmit nonpublic university information in any format or media.

OVERVIEW

The Information Security Program (Program) describes Brigham Young University's approach to protecting nonpublic university information in support of the Information Security and Appropriate Use Policy. The primary objectives of the program are to 1) provide reasonable assurance nonpublic university information will be protected from unauthorized access, use, modification, or disclosure; and 2) comply with applicable state and federal laws and contractual agreements. Protecting nonpublic university information is a shared responsibility between the Office of Information Technology (OIT) and all university departments.

ASSESSING INFORMATION SECURITY RISKS

The university recognizes it may be subject to common internal and external information security risks that include, but are not limited to, the following:

- Unauthorized access to information by someone other than the owner of the information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into information systems
- Corruption of data or systems
- Unauthorized access to information by employees
- Unauthorized requests for information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of information through third parties
- Lost or stolen laptops and other portable devices

Additionally, the Office of Information Technology (OIT) actively monitors security advisories from authoritative sources such as Educause, REN-ISAC, SANS, etc. to keep apprised of new security risks. Best practice frameworks such as the Center for Internet Security, NIST, ISO, are also used to help assess risks and improve the Program.

IMPLEMENTING SAFEGUARDS

Risk Based Implementation

The level of administrative and technical safeguards implemented will depend on

- The risk classification of the information or information system needing protection (see the CES Information and Risk Classification standard), and
- The nature, likelihood, and potential impact of the risks identified above.

Thus, information with a higher risk classification is expected to have a higher level of protection.

Limiting Access
Access to nonpublic university information is to be granted only in accordance with the Information Technology: Information Security and Appropriate Use Policy.

Employee Management and Training

Background Checks
Background checks are to be performed on all new employees that work with *highly confidential*[1] information (e.g., Cashier's Office, Registrar's Office, Student Financial Services, OIT, etc).

Security Training
Employees that work with nonpublic university information are to receive training on the importance of confidentiality of student records, student financial information, and other types of sensitive information. Training will address topics such as

- proper use of computer information and passwords,
- proper handling of *highly confidential* data,
- controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling,"[2]
- how to properly dispose of documents that contain *highly confidential* information, and
- how to protect information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.
- Restrictions concerning sharing of data with third parties

University departments that maintain information classified as *highly confidential* will regularly coordinate with the responsible Information Steward and Compliance Coordinator on any additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard information.

Physical Security
Critical IT systems are to be physically secured in rooms that allow access only to authorized users. Visitors, contractors, and vendor service personnel are required to register and be escorted by authorized university personnel when accessing these systems. Information on critical systems is to be backed up to a remote location and readily accessible.

Paper documents with nonpublic university information are to be kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees are provided with the needed combinations and the location of keys. Paper documents that contain nonpublic university information are to be shredded at time of disposal.

Information Systems Security
University departments are to take reasonable and appropriate steps to ensure that all nonpublic information is secured while stored, processed, and transmitted.

Servers
Servers are required to comply with approved information security standards and procedures. These requirements include but are not limited to the following:

- Secure configurations
- Maintaining operating system and application patches and updates in a timely fashion
- Proper administrative access controls
- User and system passwords compliant with university password standards

Firewalls and Intrusion Detection Systems
All information is to be maintained on servers that are behind the university's firewall. All firewall software and hardware is to be kept current. In addition, an intrusion detection system is implemented to detect and

[1] See the CES Information and Risk Classification Standard

[2] "Pretext calling" occurs when an individual improperly obtains personal information of university customers so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the University to release customer identifying information.

stop certain external threats.

Encryption
When commercially reasonable or required by law or contract, encryption technology will be utilized for both storage and transmission of nonpublic university information.

Selection of Appropriate Service Providers
In choosing a service provider that will maintain or regularly access nonpublic university information, university departments are to assess a service provider's ability to safeguard non-public information according to university information security standards. For service providers who maintain or access information classified as *highly confidential*, departments are to have a formal contract in place with provisions that adequately protect the confidentiality, integrity, and availability of the information. Provisions to consider include, but are not limited to, the following:

- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than the university protects its own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the university to terminate the contract without penalty; and
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

DEVELOPING POLICIES, STANDARDS, AND PROCEDURES

University-wide policies, standards, and procedures associated with this Program are to be developed and maintained by OIT. Departments should develop standards and procedures as needed to implement the provisions of this Program.

Information Security Incident Response Plan
OIT will implement processes and procedures to detect actual or attempted attacks on university systems and will implement a security incident response plan that outlines procedures for responding to an actual or attempted unauthorized access to information. This plan will be maintained by the OIT Information Security Officer.

ADJUSTING THE PLAN

This plan is subject to periodic review and adjustment as needed to reflect any changes in technology, the sensitivity of the information and internal or external threats to information security. The Information Security Officer, in consultation with the Office of General Counsel, and the Information Security and Privacy Committee (ISPC) will review this Program and recommend updates and revisions to the CIO.

ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)—provides management oversight of the Information Security Program.

Information Security Officer (ISO)—is the designated coordinator of the security program and is responsible for development, implementation, and on-going maintenance.

Information Security and Privacy Committee–-provides additional guidance regarding the university's security and privacy needs as an advisory committee to the University's Enterprise Risk Management and Compliance Committee.

Information Stewards—have direct operational-level responsibility for the management of institutional information within their area of responsibility—its security, quality, and availability. This includes recommending the classification of data based on its sensitivity and risk to the institution, reviewing and approving access to information within their domain, overseeing business continuity plan and their unit's plan and response to security breaches.

University Departments--are responsible for protecting private university information in their possession according to provisions of this plan and other university information security standards and procedures.

Human Resource Services--is responsible for performing background checks on all new Administrative and Staff employees.

Faculty Relations Office--is responsible for performing background checks on all new faculty.

RELATED INFORMATION

- infosec.byu.edu (Website of university information security standards and procedures)
- CES Information and Risk Classification
- Information Security Incident Response