BOISE STATE UNIVERSITY

University Policy #8060

Information Privacy and Data Security

Effective Date

December 2006

Last Revision Date

October 2013

Responsible Party

Associate Vice President and Chief Information Officer, (208) 426-3033
Office of Information Technology, (208) 426-4357
Chief Information Security Officer, (208) 426-5701

Scope and Audience

This policy applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers and all other entities or individuals with access to (a) confidential information through Boise State or its affiliates or (b) University information resources, including those used by the University under license, contract or other affiliation agreement.

Additional Authority

- Family Educational Rights and Privacy Act ("FERPA")
- Financial Services Modernization Act, a.k.a., the Gramm Leach Bliley Act ("GLBA")
- Health Insurance Portability and Accountability Act ("HIPAA")
- Idaho Code §28-51-105
- Payment Card Industry – Data Security Standard, Version 3.1 ("PCI-DSS")
- Idaho Public Records Act I.C § 9-377-343
- The Sarbanes-Oxley Act (Sarbanes-Oxley)
- National Institute of Standards and Technology (NIST)

- HHS 45 CFR 46 Protection of Human Subjects Subparts A-E
- University Policy 8000 (Information Technology Resource Use)

1. Policy Purpose

State a reason or rationale why the policy is needed, such as legal or regulatory requirement, risk mitigation, or general principle the university community must follow.

2. Policy Statement

This policy creates an environment that will help protect all members of the Boise State community from information security threats that could compromise privacy, productivity, reputation, or intellectual property rights. The University recognizes the vital role data and information plays in its educational and research missions, and the importance of taking the necessary steps to protect information in all forms.

3. Definitions

3.1 Access

Any personal inspection or review of the confidential information or a copy of the confidential information, or an oral or written account of such information.

3.2 Chief Information Security Officer (CISO)

The individual responsible for protecting confidential information in the custody of the University; the security of the equipment and/or repository where this information is processed and/or maintained and the related privacy rights of University students, faculty and staff concerning this information. A CISO has primary responsibility for oversight of information security, networks and systems, and working in cooperation with OIT and Human Resource Services (HRS) to educate the University community about security responsibilities.

3.3 Confidential Information

Information identified by the applicable laws, regulations or policies as personal information, individually identifiable health information, education records, personally identifiable information, non-public personal data, confidential personal information, or sensitive scientific or sponsored project information. This includes but is not limited to any information that identifies or describes an individual such as a social security number, physical description, home address, non-business telephone numbers, ethnicity, gender, signature, passport number, bank account or credit card numbers, expiration dates, security codes, passwords, educational information, medical or employment history, driver's license number, or date of birth. Also includes electronic data that includes an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or data elements are not encrypted: 1) social security number; 2) driver's license or state identification card number; 3) student or employee identification number; or 4) credit card number in combination with any required security code, access code, password or expiration number that would permit access to an individual's financial account.

Confidential information does not include any information knowingly and voluntarily made publicly available by the owner of such information, such as information voluntarily listed in public phone directories.

3.4 Custodian

Member of the University community having primary responsibility for gathering, inputting, storing, managing or disposing of confidential information. One becomes a custodian either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, for purposes of this policy, librarians have custody of library catalogs and related records, faculty have custody of their research and course materials, students have custody of their own work, and any individual who accepts a credit card number in the course of conducting University business is the custodian of that information. The term does not necessarily imply legal ownership.

3.5 Data

Information generated in the course of official University business. Information that is personal to the operator of a system and stored on a University IT resource as a result of incidental personal use is not considered University data.

3.6 Data Classification Standards

Standards used to classify University data based on sensitivity.

3.6.1 Level One Data

Private information that must be protected by law or industry regulation. Considered highly sensitive (HS).

3.6.2 Level Two Data

Information that should be protected. Considered moderately sensitive (MS).

3.6.3 Level Three Data

Publicly available information. Considered non-sensitive (NS).

3.7 Disclosure

To permit access to or release, transfer, disseminate, or otherwise communicate any part of information by any means, including but not limited to orally, in writing, or by electronic means to any person or entity.

3.8 Incident

A potentially reportable incident that may include, but is not limited to, the following:

- Attempts to gain unauthorized access to systems or data;
- Unwanted disruptions or denial of services;
- A virus outbreak;
- Theft, misuse or loss of electronic equipment containing confidential information;
- Unauthorized use of systems for processing or data storage;
- A department or unit cannot account for or fails to properly dispose of paper records containing confidential information;
- Unauthorized changes to system hardware, firmware and software.

3.9 Individually Identifiable Health Information

Any information, including demographics, collected from an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse relating to the past, present or future physical or mental health or condition of an individual and identifies the individual, or information which can reasonably be expected to identify the individual. Look for a complete list of examples.

3.10 Information Resources

Includes information in any form and recorded on any media, and all computer and communications equipment and software.

3.11 Information Service Provider (Service Providers)

A person or entity that receives, maintains, processes or otherwise is permitted to access confidential information through its provision of services directly to the University. Those colleges, departments, individuals and ancillary organizations who manage significant information resources and systems for the purpose of making those resources available to others. This includes the Office of Information Technology, Albertson's Library, the Alumni Association, University Health Services, Registrar, and Financial Aid, as well as other entities that operate at a college, division, department or sub- department level.

3.12 Level One Data

Private information that must be protected by law or industry regulation. Considered highly sensitive (HS).

3.13 Level Two Data

Information that should be protected. Considered moderately sensitive (MS).

3.14 Level Three Data

Publicly available information. Considered non-sensitive (NS).

3.15 Managers

Members of the University community who have management or supervisory responsibility, including deans, department chairs, directors, department heads, group leaders, or supervisors. Includes faculty who supervise teaching or research assistants.

3.16 Minimum Security Standards for Systems

Required configuration standards, maintained by the Office of Information Technology, that increase the security of systems (servers, workstations, mobile devices) and help safeguard University information technology resources and data.

3.17 Protected Health Information (PHI)

Individually identifiable health information that is maintained in any medium or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), and records held by a covered entity in its role as an employer.

3.18 Users

Anyone who uses Boise State's information resources, even if they have no responsibility for managing the resources. Includes students, faculty, staff, contractors, consultants and temporary employees. Responsible for protecting the information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices (paper, reports, books, film, microfiche, microfilms, recordings, computers, disks, jump drives/memory sticks, printers, phones, fax machines, etc.) they use or possess. Users must follow the information security practices set by the CISO, as well as any additional departmental or other applicable information security practices.

4. Responsibilities and Procedures

4.1 Data Classifications (Reference Data Classification Standards)

University data is classified among three levels: One, Two, and Three. All data, regardless of classification, must be protected as per the University's Minimum Security Standards for Systems.

4.1.1 Level One (Highly Sensitive, HS) Data

This is the most sensitive data that must never be left unattended without being properly secured. This includes University data protected by:

- Federal or State law (for example, HIPAA; FERPA; Sarbanes-Oxley; Gramm-Leach-Bliley; and HHS 45 CFR 46 Protection of Human Subjects Subparts A-E);
- Industry Regulation (for example, PCI-DSS);
- University rules and regulations;
- Contractual agreements requiring confidentiality, integrity, or availability considerations (for example, Non-Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements).

4.1.2 Level Two (Moderately Sensitive, MS) Data

This data includes internal data used for official University business. While there might not be a specific statute requiring its protection, this data should be safeguarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use.

4.1.3 Level Three (Non-Sensitive, NS) Data

This data includes information that may or must be open to the public and has no existing local, national or international legal restrictions on access or usage.

4.2 Security Protection Measures

All employees are required to fulfill annual security awareness training as provided and administered by the Office of Information Technology at the direction of the CISO and in support of this policy.

Detailed security measures for protecting data can be found at Minimum Security Standard for Systems. Additionally:

- Questions about this standard should be addressed to the Chief Information Security Officer.
- Questions about properly classifying specific pieces of information should be addressed to department managers, or by learning How to Classify Data.
- University data stored on non-University IT resources must still be verifiably protected as per the University's Minimum Security Standards.

4.3 Group Responsibilities

All members of the University community share in the responsibility for protecting information resources for which they have access or custody. Responsibilities set forth in this section are assigned to four groups: Custodians, Users, Managers (of users), and Information Service Providers. Individuals may have responsibilities in more than one area and should be familiar with the requirements of each group.

4.3.1 Custodian Responsibilities

- Establishing information security procedures.
- Determining Authorizations.
- Recordkeeping
- Incident handling and reporting (view Custodian Data Security Guidelines)

4.3.2 User Responsibilities

- Adhering to University IT policies
- Physical security
- Information storage
- Distribution and transmission of information
- Destruction and disposal of information and devices
- Passwords
- Computer security
- Remote access
- Logging off
- Virus and malicious code protection
- Backups
- Incident handling and reporting (view User Data Security Guidelines)

4.3.3 Manager Responsibilities

- Everything users are responsible for
- Everything custodians are responsible for including the origination and mechanisms for information resource sharing
- Sharing responsibility for information security with the employees they supervise
- Establishing information security procedures
- Managing authorizations
- User training and awareness

- Physical security
- Incident handling and reporting (view Manager Data Security Guidelines)

4.3.4 Information Service Provider Responsibilities

- More extensive information security requirements than individuals
- Establishing information security procedures
- Physical security
- Computer security
- Network security
- Access controls
- Passwords
- Contingency planning
- Incident handling and reporting (view Information Service Provider Data Security Guidelines)

4.4 Administrative Responsibilities

The CISO continually monitors the University information security threat landscape and proposes tools or mitigation strategies to reduce the University's exposure. Oversight and responsibilities include:

- Creating, reviewing, and revising policies, procedures, standards.
- Ensuring security training and awareness.
- Overall authority for University networks and systems security.
- Incident handling, remediation, and reporting.
- Collaborating with the Office of Internal Audit to ensure policy conformance. (View CISO Data Security Guidelines).

4.4.1 Office of General Counsel Responsibilities

The Office of General Counsel (OGC) is responsible for interpreting the laws that apply to this policy and ensuring that the policy is consistent with those laws and other University policies. Any inadequacies in this policy should be brought to the attention of the CISO. The OGC will work in concert with the CISO and other parties deemed necessary to report any criminal offenses when necessary.

4.4.2 Office of Information Technology Responsibilities

The Office of Information Technology (OIT) is responsible for working with the CISO to develop standards consistent with this policy, other University policies, and state and federal law. OIT will also work with the CISO to assist with training and compliance issues.

4.5 Enforcement

Violations of this policy will be handled consistent with University disciplinary procedures applicable to the relevant individuals or departments. Failure to comply with this policy may also result in the suspension of access to network resources until policy standards have been met. Should Boise State incur monetary fines or other incidental expenses from security breaches, the University may recoup these costs from the non-compliant department, school or auxiliary organization.

5.0 Related Information

Minimum Security Standards for Systems
https://www.boisestate.edu/oit-itgrc/it-standards-category/boise-state-university-minimum-security-standards-for-systems/

Data Classification Standards
https://www.boisestate.edu/oit-itgrc/it-standards-category/boise-state-university-data-classification-standard-2/

How to Classify Data
https://www.boisestate.edu/oit-itgrc/examples-of-how-to-classify-data/

Minimum Security Standards
https://www.boisestate.edu/oit-itgrc/it-standards-category/boise-state-university-minimum-security-standards-for-systems/

Incident Handling and Reporting
https://www.boisestate.edu/oit-itgrc/it-plans-procedures-category/boise-state-university-information-technology-incident-response-procedure/

Custodian Data Security Standards
https://www.boisestate.edu/oit-itgrc/

User Data Security Guidelines
https://www.boisestate.edu/oit-itgrc/users-data-security-guidelines/

Manager Data Security Guidelines
https://www.boisestate.edu/oit-itgrc/users-data-security-guidelines/

Information Service Provider Data Security Guidelines
https://www.boisestate.edu/oit-itgrc/policy-8060-data-isp-detail/

CISCO Data Security Guidelines
https://policy.boisestate.edu/information-technology/policy-title-information-privacy-and-data-security/

Revision History

October 2013; September 2016