BOISE STATE UNIVERSITY

University Policy 8060

Information Privacy and Data Security

Effective Date

December 2006

Last Revision Date

March 29, 2023

Responsible Party

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")
- The Sarbanes-Oxley Act (Sarbanes-Oxley)
- Arms Export Control Act ("AECA")
- International Emergency Economic Powers Act ("IEEPA")
- Export Controls Reform Act ("ECRA")
- Payment Card Industry – Data Security Standard, Version 3.1 ("PCI-DSS")
- National Institute of Standards and Technology (NIST)

- 45 CFR Part 46 Protection of Human Subjects Subparts A-E
- Idaho Code § 28-51-105
- 32 CFR Part 2002 Controlled Unclassified Information ("CUI")
- Idaho Code Title 74, Chapter 1 (Idaho Public Records Act) University Policy 8000 (Information Technology Resource Use)

1. Policy Purpose

To classify Data and establish minimum standards and guidelines to protect against accidental or intentional damage or loss of Data, interruption of University business, or the compromise of Confidential Information.

2. Policy Statement

Boise State University strives to create a security framework that will ensure protection from information security threats that could compromise privacy, productivity, reputation, or intellectual property rights. The university recognizes the vital role that Data and information play in its educational and research mission 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 Confidential Information, or a copy of 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 such information is processed and/or maintained, and the related privacy rights of University students, faculty, and staff concerning such information. The CISO has primary responsibility for oversight of information security, networks and systems, and working in cooperation with OIT and Human Resources to educate the University community about security responsibilities.

3.3 Confidential Information

Information identified by the applicable laws, regulations, or policies as personal information, including:

- Protected Health Information (PHI), as well as Personally-Identifiable Health Information;
- Education records, personally identifiable information (PII);
- Non-public personal Data;
- Controlled unclassified information (CUI);
- Export controlled information (ECI);
- Covered defense information;
- 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.

This 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 the 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

Members of the University community having primary responsibility for gathering, inputting, storing, managing, or disposing of confidential information. An individual 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 used 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 Incident

A potentially reportable event 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's inability to account for or properly dispose of paper records containing Confidential Information; or
- Unauthorized changes to system hardware, firmware, and software.

3.7 Information Resources

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

3.8 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, Albertsons Library, the Alumni Association, University Health Services, Registrar's Office, Financial Aid, and any other entity operating at a college, division, department, or sub- department level.

3.9 Managers

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

3.10 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.

3.11 Users

Anyone who uses Boise State's Information Resources, even if the individual has no responsibility for managing such resources. This includes students, faculty, staff, contractors, consultants, and temporary employees responsible for protecting the Information Resources to which they have Access. User 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. Data Classifications

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

4.1 Level One (Highly Sensitive, "HS") Data

Level One Data must be protected as specifically guided by law (e.g., HIPAA, FERPA, Sarbanes-Oxley, Gramm-Leach-Bliley), industry regulation (PCI-DSS), government controls (CUI, FISMA), or University rules and regulations (contracts, MOUs). This is the most sensitive Data of the university and must be safeguarded.

4.2 Level Two (Moderately Sensitive, "MS") Data

Level Two Data is proprietary Data, but which is generally releasable in accordance with the Idaho Public Records Act. Such Data must be appropriately protected to ensure a controlled and lawful release. This Data includes internal Data used for official University business and must be

safeguarded due to proprietary, ethical, or privacy considerations and protected from unauthorized Access, modification, transmission, storage, or other use. Applicable privacy laws will be considered before release of Data.

4.3 Level Three (Non-Sensitive, "NS") Data

Level Three Data is generally publicly available Data and considered non-sensitive. Such Data have no requirements for confidentiality, integrity, or availability.

5. Security Protection Measures

All employees are required to fulfill annual security awareness training as provided and administered by the State of Idaho.

Detailed security measures for protecting Data can be found on the OIT website. 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 using the How to Classify Data information on the OIT website.
- University Data stored on non-University IT resources must still be verifiably protected as per the University's Minimum Security Standards for Systems.

6. Group Responsibilities

All members of the University community who have Access to or custody of Information Resources share in the responsibility for protecting such information. The responsibilities set forth in this section are assigned to four groups: Custodians, Users, Managers, and Information Service Providers. Individuals may have responsibilities in more than one area and should be familiar with the requirements of each group. Laws and regulations governing Tier 1 Data may call out specific requirements for each of these groups.

6.1 Custodian Responsibilities

- Establishing information security procedures
- Determining authorizations
- Recordkeeping

- Incident handling and reporting
- Following Incident Response Procedures

6.2 User Responsibilities

- Adhering to University IT policies
- Ensuring physical security of Data
- Ensuring appropriate storage of information
- Ensuring the appropriate distribution and transmission of information
- Properly destroying and disposing of information and devices
- Protecting passwords
- Ensuring computer security
- Adhering to remote Access security protocols
- Logging out of systems and applications when not in use and locking workstations prior to leaving the work area
- Protecting information from virus and malicious codes
- Performing information backups (see Minimum Standards for Desktops and Software)
- Following Incident Response Procedures

6.3 Manager Responsibilities

- Managing User responsibilities
- Managing Custodian responsibilities, 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

- Ensuring their employees complete all required User training and awareness
- Ensuring physical security of information
- Following Incident Response Procedures

6.4 Information Service Provider Responsibilities

- Information service providers have more extensive information security requirements than individuals, including but not limited to:
- Establishing information security procedures
- Ensuring physical security
- Ensuring computer security
- Ensuring network security
- Maintaining Access controls
- Protecting passwords
- Using NIST-compliant encryption methods for Level One Data as specified in the Minimum Security Standards
- Participating in contingency planning
- Following Incident Response Procedures

7. 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
- Overseeing University networks and systems security
- Following Incident Response Procedures

- Collaborating with Internal Audit and Advisory Services to ensure policy conformance

8. 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.

9. Office of Information Technology Responsibilities

The Office of Information Technology 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.

10. Enforcement

a. 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.

b. All data security breaches must be reported to the CISO, the Office of Risk Management and Insurance, the Office of Institutional Compliance and Ethics, and the Office of General Counsel. 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.

11. Related Information

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

Data Classification Standards
https://www.boisestate.edu/oit/itgrc/it-standards/data-classification-standards/

Incident Handling and Reporting
https://www.boisestate.edu/oit/itgrc/it-plans-procedures/it-incident-response-procedure/

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

University Policy 1150 (HIPAA Hybrid Entity Designation)

University Policy 2250 (Student Privacy and Release of Information)

Revision History

October 2013; September 2016; March 29, 2023