BOISE STATE UNIVERSITY

University Policy 8060

Information Privacy and Data Security

Effective Date

December 2006

Last Revision Date

October 14, 2024

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.) Protected 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)
- 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
- General Data Protection Regulation ("GDPR")
- Idaho Code § 28-51-105

- Idaho Code Title 74, Chapter 1 (Idaho Public Records Act)
- University Policy 1020 (Public Records Management)
- University Policy 1090 (Intellectual Property)
- University Policy 1150 (HIPAA Hybrid Entity Designation)
- University Policy 2250 (Student Privacy and Release of Information)
- University Policy 5120 (Export Control and Controlled Data)
- University Policy 8000 (Information Technology Resource Use)
- University Policy 8160 (Data Governance Committee)
- University Policy 11050 (Donor Records)
- University Policy DRAFT (Research Data Management)

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 Protected 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, confidentiality, availability, security, or intellectual property rights. The university recognizes the vital role that Data and information play in its educational, research, and creative activity 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 Confidential Information, or a copy of Protected Information, or an oral or written account of such information.

3.2 Chief Information Security Officer (CISO)

The individual responsible for securing Protected 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 the Office of Information Technology

(OIT), the Division of Research and Economic Development (DRED), the Registrar's Office, Admissions, and Human Resources and Workforce Strategy to educate the University community about security responsibilities.

3.3 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.

3.4 Data Custodian

Members of the University community with primary responsibility for the technical control of Data to include gathering, inputting, storing, managing, or disposing of Protected Information. An individual becomes a Data 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 Data Custodian of that information. The term does not necessarily imply legal ownership.

3.5 Data Owner

Members of the University community who are primary decision-makers, ultimately accountable for the classification, protection, use, and quality of one or more Data sets within their purview, including the application of relevant policy to the respective Data. This Data may or may not be produced by the university and may also include research information provided by another institution. The Data Owner assesses and manages the risks associated with the data in their domain, having both the authority and access to make and approve changes to ensure Data quality; as well as authorizing others to do so. Data Owners may also exercise judgment to determine when it is appropriate to increase or decrease a classification level when the guidelines are not straightforward. Due to the critical nature of their role, the Data Owner is typically the senior member of their respective department or division.

3.6 Data Steward

Members of the University community with primary responsibility for the business controls, data content, and quality of defined data assets. Typically, the data steward is the Subject Matter Expert (SME) who understands the importance of a set of Data and how that Data should be curated. Stewards work with stakeholders who are impacted by data to develop definitions,

standards, classifications, and controls. In some instances, the Data Steward and Data Custodian may be the same person.

3.7 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 computer virus outbreak;
- Theft, misuse, or loss of electronic equipment containing Restricted or 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 Restricted or Protected Information; or
- Unauthorized changes to system hardware, firmware, and software.

3.8 Information Resources

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

3.9 Information Service Provider (Service Providers)

Colleges, departments, individuals, or outsourced organizations responsible for managing Information Resources and/or systems for the purpose of making such resources available to others.

3.10 Managers

Members of the University community with 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.

3.11 Minimum Security Standards for Systems

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

3.12 Protected Information

Information identified by the applicable laws, regulations, or policies as sensitive information, including but not limited to:

- Protected Health Information (PHI), as well as Personally-Identifiable Health Information;
- Education records;
- Personally identifiable information (PII);
- Controlled unclassified information (CUI);
- Export controlled information (ECI);
- Covered Defense Information (CDI);
- Non-Disclosure Agreements (NDA) with third parties;
- Confidential 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, debit or credit card 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 (1) r 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.

Protected 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.

Additional information regarding data definitions and restrictions can be found in University Policy 5120 (Export Control and Controlled Data).

3.13 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 (e.g., 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 four levels: Restricted, Confidential, Internal, and Public. All Data, regardless of classification, must be protected as per the University's Minimum Security Standards for Systems. Specific examples are contained within the University's Data Use Guidelines.

4.1 Restricted Data

Restricted Data is sensitive data intended for limited, specific use and must be protected as specifically guided by law (e.g., HIPAA, FERPA, Sarbanes-Oxley, Gramm-Leach-Bliley), industry regulation (PCI-DSS), government controls (CUI, ECI, FISMA, CDI), Non-Disclosure Agreements (NDA), or University rules and regulations. This is the most sensitive Data of the university and must be safeguarded in accordance with its individual requirements (i.e., some Restricted Data require more rigorous controls than other Restricted Data).

4.2 Confidential Data

Confidential Data is intended for limited University business use only, with access restricted to personnel with a legitimate need, even though that need may constitute a small group (e.g., only designated security personnel) or a large group (e.g., all student advisors or all faculty). This classification also includes Data that is not subject to public disclosure and that the University is

required to keep confidential per legal agreements, policies, or third-party agreements such as vendor contracts and MOUs.

4.3 Internal Data

Internal Data is information used for official University business and must be safeguarded due to ethical or privacy considerations and protected from unauthorized Access, modification, transmission, storage, or other use. This Data is not intended to be shared with the public; however, it is generally releasable in accordance with the Idaho Public Records Act. This Data includes potentially sensitive information and applicable privacy laws will be considered before release of Data.

4.4 Public Data

Public Data is generally explicitly or implicitly approved for distribution to the public without restriction and is considered non-sensitive. Such Data will have no requirements for confidentiality, integrity, or availability.

5. Security Protection Measures

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

b. Detailed security measures for protecting Data can be found on the OIT website. Additionally:

- Questions about this standard should be addressed to the CISO.
- Questions about properly classifying specific pieces of information should be addressed to department Managers, Data Owners, or by following the University Data Use Guidelines 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 six groups: Data Owners, Data Custodians, Data Stewards, Users, Managers, and Information Service Providers. Individuals may have responsibilities in

more than one (1) area and should be familiar with the requirements of each group. Laws and regulations Restricted Data may call out specific requirements for each of these groups.

6.1 Data Owner Responsibilities

- Managing Data Custodian and Data Steward responsibilities, including the origination and mechanisms for information resource sharing
- Determining the classification of data
- Setting the overall direction for data quality and usage
- Determining access and authorization to data
- Ensuring the data complies with regulations
- Ensuring the physical security of information
- Following Incident Response Procedures

6.2 Data Custodian Responsibilities

- Establishing information security procedures to prevent the data from unauthorized access
- Determining authorizations with Data Owner guidance
- Recordkeeping
- Following Incident Response Procedures

6.3 Data Steward Responsibilities

- Creating data definitions and describing allowed values
- Defining rules for data generation, data usage, or data derivatives
- Assessing and documenting current and desired data systems
- Establishing data quality objectives
- Advocating for the proper use of data within the university

- Following Incident Response Procedures

6.4 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
- 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 passwords
- Protecting information from virus and malicious codes
- Performing information backups (see Minimum Standards for Desktops and Software)
- Following Incident Response Procedures

6.5 Manager Responsibilities

- Managing User responsibilities
- Sharing responsibility for information security with the employees they supervise
- Establishing information security procedures for their department or unit
- Managing authorizations
- Ensuring their employees complete all required User training and awareness
- Ensuring physical security of information

- Following Incident Response Procedures

6.6 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 established by the Data Custodian and University
- Periodically review User identifiers and access privileges and revise them as required
- Protecting passwords
- Using industry and regulatory compliant encryption methods (e.g., AES 256 or equivalent) for Restricted Data as specified in the Minimum Security Standards and NIST SP 800-171 Rev. 2)
- 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, and 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
- Serving as a member of the Data Governance Committee

8. Data Governance Committee Responsibilities

The Data Governance Committee (DGC) is the managing authority for the establishment of University operating standards, policies, and values to promote and guide effective and responsible data governance covering the following areas (see also University Policy 8160 - Data Governance Committee):

- Data Access
- Data Use
- Data Quality
- Data and Record Retention

9. 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.

10. Division of Research and Economic Development

The Division of Research and Economic Development (DRED) provides comprehensive support for faculty, staff, and student research and creative activity, ensuring the University's intellectual property portfolio meets with the specifications in this and other University policies. DRED will work in concert with the CISO and other parties necessary regarding security and Data types under their purview (e.g., CUI, including PHI, ECI, and CDI).

11. 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.

12.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 suspected data security breaches must be reported to the CISO at CISO@boisestate.edu, by calling (208) 426-4127, or through a Help Desk request. The CISO will then coordinate as needed with Risk Management and Insurance, the Office of Institutional Compliance and Ethics, the Office of General Counsel, and the Division of Research and Economic Development (DRED). Should Boise State University incur monetary fines or other incidental expenses from security breaches, the university may recoup these costs from the non-compliant department, division, college or school, or auxiliary organization.

13. Related Information

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

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

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

Revision History

October 2013; September 2016; March 29, 2023; October 14, 2024