
INFORMATION PRIVACY AND SECURITY

Purpose:

To 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.

Additional References:

Family Educational Rights and Privacy Act ("FERPA"), Gramm Leach Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), Idaho Code § 28-51-105, Payment Card Industry ("PCI") Data Security Standard, Version 1.1

Scope:

Applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers and all other entities or individuals with access to confidential information through Boise State or its affiliates.

This policy applies to all university information resources, including those used by the university under license or contract.

Responsible Party:

Information Security Officer, 426-1159

Definitions:

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.

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

Confidential Information – Any information identified by the applicable laws, regulations or policies as personal information, individually identifiable health information, confidential information, education records, personally identifiable information, non-public personal data, confidential personal information, or sensitive 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.

Confidential information also refers to 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 the 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.

CVV2 – security code on credit cards used to process transactions by phone, online, or in other instances where the cardholder is not conducting a transaction in person.

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

- An employee, contractor, or third-party obtains unauthorized access to confidential information in either paper or electronic form;
- An intruder accesses a database containing confidential information on an individual;
- A virus outbreak;
- Computer equipment such as a workstation, laptop, CD or other electronic media containing confidential information has been lost or stolen;
- A department or unit cannot account for or fails to properly dispose of paper records containing confidential information;
- A third party service provider experiences any of the incidents described above.

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.

Information Resources – includes information in any form and recorded on any media, and all computer and communications equipment and software.

Information Security Officer (“ISO”) – the individual or individuals 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.

Information Service Provider – any person or entity that receives, maintains, processes or otherwise is permitted to access confidential information through its provision of services directly to the university.

Third Party – any individual acting alone or on behalf of an organization who is not an employee of Boise State University.

Track 1 Data – Data stored on the magnet strip of a credit card including cardholder’s name, account number and other discretionary data.

Track 2 Data – Data stored on the magnet strip of a credit card that is read by ATMs and credit card machines. Stored data includes cardholder account information, encrypted PIN and other discretionary data.

POLICY

I. Policy Statement

- A. The Boise State University Information Privacy and Security Policy serves to create an environment which 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 information plays in its educational and research missions, and the importance of taking the necessary steps to protect information in all forms. As more information is used and shared by students, faculty and staff, both within and outside the university, a concomitant effort must be made to protect information resources from threats by establishing responsibilities, guidelines, and practices that will help the university prevent, deter, detect, respond to and recover from compromises to these resources.

II. Responsibilities

- A. 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.
 - 1. Custodians – those members of the university community who have 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 custody does not necessarily imply legal ownership. In fact, information housed on university computers or networks may be legally owned by an entity outside the university, as with licensed software.

Custodians are responsible for:

- a. **Establishing information security procedures.** Custodians must establish internal standards and procedures relating to the creation, retention, distribution and disposal of information. These standards must meet the minimum standards set by the ISO, the university's records retention policy, as well as other university policies, contractual agreements, and governing federal, state and local laws. Custodians may impose additional requirements to enhance security as long as they are consistent with the above authorities.
- b. **Determining Authorizations.** Custodians must determine who is authorized to have access to their information. They must ensure that those with access have a need to know the information and understand the security requirements for that information. Where applicable, custodians must ensure that those with access to confidential information have signed a confidentiality agreement covering the information they are responsible for.
- c. **Recordkeeping.** Custodians must keep records documenting the creation, distribution and disposal of all confidential information.
- d. **Incident Reporting.** Custodians must report suspected or known compromises of their information to their managers and the ISO on the same business day that they become aware of the compromise. The ISO will proceed in accordance with the Incident Response

Procedure.

2. Users – all members of the university community are users of Boise State’s information resources, even if they have no responsibility for managing the resources. Users include students, faculty, staff, contractors, consultants and temporary employees. Users are 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, PDAs, disks, jump drives/memory sticks, printers, phones, fax machines, etc.) that they use or possess. Users must follow the information security practices set by the ISO, as well as any additional departmental or other applicable information security practices.

Users are responsible for:

- a. **Being familiar with and adhering to university policies.** Users are expected to adhere to all university policies and exercise good judgment in the protection of information resources. They should be familiar with this policy and other information-related policies, including but not limited to the university’s policies regarding acceptable use, access and privacy.
- b. **Physical security.** Users must provide physical security for their information technology devices. Doors must be locked to protect equipment when areas housing them are unattended. Special care should be exercised with portable devices which are vulnerable to loss or theft.
- c. **Information storage.** Confidential information must be kept in a place that provides a high level of protection against unauthorized access and should not be removed from the university. Encryption consistent with university standards is required for confidential information stored electronically on all computers, and special care should be taken when electing to store confidential information on laptops, PDAs, or other devices that are vulnerable to theft or loss.
- d. **Distribution and transmission of information.** Confidential information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception.

For electronic information, appropriate encryption is required for all restricted information, especially if that information is transmitted over public networks. Information Services Providers are responsible for employing appropriate encryption when transmitting electronic information; users must avail themselves of these services.

- e. **Destruction and disposal of information and devices.** Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents containing confidential information must be shredded prior to disposal.

When donating, selling, transferring, or disposing of computers or removable media such as jump drives, or CDs, care must be taken to ensure that confidential data is rendered unreadable. For example, if used computers are donated or sold, all information stored on machines must be thoroughly erased. It is insufficient to “delete” the information, as it may remain on the medium. Software that rewrites random data on the medium (preferably several times) must be used. Alternatively, the medium may be physically or electromagnetically destroyed.

- f. **Passwords.** Access to computers, software applications and electronic information is frequently password controlled. Users are responsible for creating and protecting passwords that grant them access to resources. Passwords cannot be shared, displayed in plain view, or stored in computers. Although different applications may have unique password requirements, passwords should generally be at least 8 characters long and include a combination of letters, numbers, and symbols. Passwords should not contain names, words, or permutations of personal data such as social security numbers, dates of birth, etc. Passwords must be changed at least every 90 days, and default passwords must be changed on a user’s first login.
- g. **Computer security.** Users must take steps to protect their desktop, laptop, and PDAs from compromise either by external individuals or members of the university

community. Users must utilize secure operating systems and software and modify default installation passwords and configurations to minimize vulnerabilities. It is the user's responsibility to ensure that security patches are promptly installed on their laptop, desktop and/or PDA, or to ensure that an Information Service Provider has installed these patches. Users must cooperate with and avail themselves of any central services providing support for and/or review of these activities.

- h. **Remote access.** Many personal computer operating systems can be configured to allow access across the Internet and other networks. Users must ensure their systems are configured to prevent unauthorized access.
- i. **Log off.** Users must log off of applications, computers and networks when finished. If computers are located in secure locations, users may not leave without locking office doors, regardless of the time they anticipate being away. Public terminal users must also log off when completing their session. The use of boot or start-up passwords is required where unauthorized users may have physical access to computers. Users should activate their auto-off monitor function, which requires a password to reactivate.
- j. **Virus and Malicious Code Protection.** Users must ensure that their personal computers employ mechanisms that protect against viruses and other forms of malicious code which may be distributed through email or the web. Users must have anti-viral software loaded on any device used to access the university's network from off-site. To ensure that virus protection remains effective, individuals must install new versions as they become available.

Because no anti-viral software is effective against all viruses, users must exercise caution when opening email or downloading files from the Internet. Users should not open unexpected or suspicious attachments and should configure word processing, spreadsheet, and other applications to require user confirmation before macros, scripts, or other executable enclosures are opened. Confirmation should be granted only if the source of the file is known or trusted.

If a virus is detected, it must be immediately and

completely eradicated before email or files of any sort are sent to other users. After contamination is eliminated, individuals who may have been sent infected files must be informed by telephone or other non-electronic means. All potentially infected files, including those stored on network servers and backup media must also be examined for infestation and treated accordingly.

For additional information, see the BSU Software Patch Management policy.

- k. **Backups.** Backups and record retention must comply with the university's records retention policy. Information stored on personal computers and not easily replaced must be copied to removable media to protect from loss. Backup copies should be made regularly and maintained in a different physical location to protect against loss from flood, fire or theft. Care should be taken to store media under environmentally appropriate, secure conditions and should be periodically refreshed.
 - l. **Incident handling and reporting.** Users must report suspected compromises of information resources, including contamination by computer viruses, to their managers and the ISO, who will proceed in accordance with the Incident Response Procedure. Incidents must be reported on the same business day users become aware of the compromise.
3. **Managers** – Managers are members of the university community who have management or supervisory responsibility, including deans, department chairs, directors, department heads, group leaders, or supervisors. Faculty who supervise teaching or research assistants are also included.

Managers have all the responsibilities of users, and where information resources originate, custodians. Additionally, they share responsibility for information security with the employees they supervise.

Managers are also responsible for:

- a. **Establishing information security procedures.** If managers elect to establish more restrictive information security practices for their employees, they must be consistent with the ISO's standards, university policies,

contractual agreements, and governing laws.

- b. **Managing authorizations.** Managers must make sure their employees have the authorizations necessary to perform their jobs. The authorizations themselves are acquired from the custodians of the information resources. Managers must ensure that employee access is consistent with employee responsibilities and that requests to deactivate employee accounts are made within 24 hours of an employee's separation.
 - c. **User training and awareness.** Managers must promote security by ensuring that employees have the training and tools necessary to protect information.
 - d. **Physical security.** Managers must ensure the physical security of the information technology devices in their area. Doors should be locked to protect equipment when unattended. Portable equipment such as laptops, PDAs and cell phones should be registered and regularly inventoried at the department level.
 - e. **Incident handling and reporting.** Managers must report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their managers and the ISO. Incidents must be reported on the same business day a manager learns a compromise has occurred. Managers must cooperate with the investigation of and recovery from security incidents, including taking any disciplinary action deemed necessary by the appropriate university authorities.
4. Information Service Providers ("Service Providers") – Service Providers are 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, Registrar, and Financial Aid, as well as other entities that operate at a college, division, department or sub-department level.

Service Providers face more extensive information security requirements than individuals. Beyond controlling access and protecting against physical threats, they must play a more

proactive role implementing and enforcing security policies and procedures, auditing access, threats, and vulnerabilities, and developing or conforming to university access, authentication, and authorization standards and practices.

Service providers are responsible for:

- a. **Establishing information security procedures.**
Service providers must establish specific information security procedures governing the information resources they manage. These procedures must meet the minimum standards set by the ISO and must be consistent with other university policies and governing statutes and regulations. Service Providers must designate personnel to maintain and assure the integrity of the information resources, systems and networks for which they are responsible, or assign this responsibility to the ISO. Any local personnel who take on these responsibilities must work closely with the ISO to achieve the objectives of this policy.
- b. **Physical security.** Computer systems (servers, desktops, portable devices, etc.), network components (switches, routers, etc.), the cable infrastructure and other facilities must be physically protected commensurate with the level of risk faced by the university should they be compromised. Power, temperature, water and fire monitoring devices should be used where appropriate. Locks, cameras and alarms must be installed in technology centers and closets to discourage and alert personnel to unauthorized access. Service Providers are responsible for ensuring that components required to conduct mission critical business are incorporated into the physical planning component of the university's strategic plan.
- c. **Computer security.** Service Providers must take steps to protect their servers and mainframes from compromise from either internal or external individuals or entities. They must select operating systems and other software that is securable and modify default passwords and configuration options to reduce potential vulnerabilities. Service Providers must ensure that security patches are consistently updated. They must periodically verify audit and activity logs, examine performance data, check for evidence of unauthorized access, the presence of viruses, or any other indicators of integrity loss. Service

Providers must cooperate with and avail themselves of any central services providing support for and/or review of these activities as well as performing more sophisticated procedures such as penetration testing and real-time intrusion detection.

Service Providers who develop, maintain, or modify key applications relating to financial data, human resources, student records, etc., must deploy adequate procedures for change control, separation of test and production environments, and separation of responsibilities for staff involved in these functions. They must proactively cooperate with Internal Audit and the Office of Information Technology to ensure that policies are respected and that adequate procedures are in place.

- d. **Network security.** Service Providers who support authorized access to university information must implement designs, policies, and procedures that protect the integrity of those services. Network security should be maintained through a combination of technologies including switched networks, strong authentication requirements, encryption and firewalls. Network access, including modem and other remote access, must be implemented using university standards for hardware, software, authentication protocols, and access controls.

Because the loss of integrity of any device or server on the network provides a platform for launching attacks on the entire network, the Information Security Officer, in concert with the Offices of Information Technology and Internal Audit will periodically probe the network and network servers for vulnerabilities, using software tools designed for this purpose. Service Providers are expected to participate in and cooperate with this process, review reports, and take corrective actions where necessary.

- e. **Access Controls.** In granting individuals access privileges to information resources, Service Providers must adhere to policies established by the data custodians and the university. Protocols specifying access authorizations must be produced in a format conducive to auditing and audit trails must be maintained at appropriate levels. User identifiers must respect the centrally generated assignments, and systems and

applications must support available university-wide standards and facilities supporting authentication, authorization, and single sign-on.

Shared, guest and anonymous accounts should be avoided. Guests must be incorporated into the central user identifier facility when possible. Any anonymous accounts must be restricted to servers containing unrestricted data and not residing within a zone protected by a firewall.

Service Providers shall periodically review user identifiers and access privileges and revise them as required by changes in job functions, transfers and employment status. Where university-wide facilities are deployed to aid user identifier management, individual systems and applications should interface with them whenever possible.

- f. **Passwords.** When passwords are used for authentication, Service Providers should install password mechanisms that provide strong security while aiding users with the selection and management of strong passwords. Where independent password files must be maintained, they must be protected by encryption and access controls. Appropriate restrictions regarding password lengths and the use of personal data or dictionary words for passwords must be implemented, using software enforcement where possible.

Initial user passwords may deviate from this only if the user is required, by the software, to change the password upon first use. Administrators and help desk personnel should be able to reset passwords following established procedures, but never able to view them. The assignment of root access or similar capabilities must be strictly controlled and very limited. Passwords to accounts with privileges that may be needed in emergency recovery situations should be made available via lock boxes rather than distributed on an anticipatory basis.

- g. **Contingency planning.** Service Providers are responsible for ensuring the continued availability of university information resources and for planning for the resumption of mission critical business information

services following the loss of equipment, data, and/or technology rooms due to flood, fire, equipment failure, natural disasters, etc. Inherent in this requirement is the need to provide effective procedures for backing up university data.

Appropriate schedules should be established for backing up servers and other devices containing important data, retaining copies, and refreshing media. Schedules and retention periods should support requirements for restoring data after accidental loss or corruption, natural disasters, and record keeping requirements as identified by the data custodians.

To ensure availability and functionality of backups, copies must be stored in secure, environmentally controlled, off-site locations. Encryption/decryption applications and copies of cryptographic keys must be stored in safe locations if they are required to restore backup data to useable form. Archived data is to be retained for legal/historical purposes and should be recopied periodically. When applications change, either the original application shall be retained so as to be able to usefully access the archived data or the archived data should be converted to a format and medium that is useable by the new or other available application.

- h. **Incident handling and reporting.** Service Providers must report suspected or known compromises of information resources to managers and the Information Security Officer, who will proceed in accordance with the Incident Response Procedure. Reporting must occur on the same business day a Service Provider learns a compromise has occurred. They must preserve and protect evidence and cooperate with any investigation. Where appropriate, they must repair vulnerabilities and impose additional security measures to protect against future compromises.

- B. Information Security Officer – The ISO 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.

The ISO is responsible for:

- a. **Policy Oversight.** The ISO must stay abreast of current legislation and how it affects security policy and planning. Additionally, the ISO must monitor activities and best practices relating to security at other institutions and follow the activities of organizations in higher education such as NACUBO and Educause.
- b. **User training and awareness.** Effective information security requires a high level of participation from all members of the university and all must be well informed of their responsibilities as information custodians, users, managers and service providers. In cooperation with managers, OIT, and Human Resources the ISO is responsible for managing a university training and awareness program for all members of the university.

The ISO must manage efforts to ensure this policy as well as related policies and procedures are distributed to the university community, using training classes and materials to instill the importance of proper information handling and explain the implications of this policy. Training should include specific information on the use of security precautions such as encryption, anti-viral tools, and backup procedures.

- c. **Oversight authority for university networks and systems.** The ISO is responsible for overseeing network and system security for resources managed by or connected to any university computer or network.
- d. **Enhancements and revisions.** In cooperation with other members of the university, the ISO must periodically reassess this policy and the related procedures to determine if revisions are needed to keep pace with the fast changing nature of information technology. If such revisions become necessary, the ISO should seek input from all relevant constituencies within the university and then propose recommended changes to the Vice President for Finance and Administration.
- e. **Incident handling and reporting.** If information resources are compromised, the university must take steps to remediate, respond to and recover from the incident. Depending on the nature of the incident, this could involve collecting and analyzing evidence, determining the responsible party, assessing damage,

restoring data from backup files, closing security holes, installing stronger security measures, revising security guidelines and procedures, taking disciplinary action in accordance with university policies, reporting incidents to law enforcement, and interacting with the media. The ISO will further investigate incidents and work with the Incident Response Team in accordance with the Incident Response Plan.

- C. Internal Audit -The ISO is responsible for working with Internal Audit to determine whether information is being protected in conformance with this policy by conducting regular audits.
 - D. University Counsel – University Counsel 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 ISO. University Counsel will work in concert with the ISO and other parties deemed necessary to report any criminal offenses when necessary.
 - E. Office of Information Technology – OIT is responsible for working with the ISO to develop standards consistent with this policy, other university policies, and state and federal law. OIT will also work with the ISO to assist with training and compliance issues.
- III. 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.

Policy adapted in part from Georgetown University's Information Security policy.