

IDAHO STATE UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES
Protection of Sensitive Data
MAPP 09.B.2

POLICY INFORMATION

Section Title: Information Technology Services

Subject: Protection of Sensitive Data

Responsible Executive: Vice President for Finance and Administration

Sponsoring Organization: Information Technology Services

Dates: Issued: August 17, 2009 Revised: _____ Annual Review: August 17, 2010

I. PURPOSE AND SCOPE

The Idaho State University (ISU) Protection of Sensitive Data policy defines and establishes the practices and standards required by the University for secure, electronic storage of sensitive data and information. Sensitive data resides on ISU's information technology (IT) systems, which may include, but are not limited to, information systems, networking and telecommunications systems, data processing hardware and software, data transmission equipment and transmission media, and data storage devices. It may also reside on department or college servers, or on individual employees' computer hard drives or other storage media. Sensitive data includes information or data processed, stored, or transmitted across ISU's IT systems, as well as department or college systems. This policy applies to all University employees and/or individuals accessing or processing University data.

The following policies are incorporated into this policy by reference:

- a. The definitions for IT policies, available at http://www.isu.edu/fs-handbook/part3/3_8/3_8a.html.
- b. The General IT Policy (http://www.isu.edu/fs-handbook/part3/3_8/3_8b.html)
- c. Faculty/Staff Handbook (<http://www.isu.edu/fs-handbook/>)
- d. Student Code of Conduct (<http://www.isu.edu/references/st.handbook/>)

II. POLICY STATEMENT

Idaho State University is strongly committed to maintaining the privacy and security of confidential personal information and other sensitive data it collects. Accordingly, the University expects all who use and/or store such information and data to treat these data with the utmost care. This expectation arises from the various University policies, federal and state laws and regulations, and contractual obligations that govern how sensitive data must be protected. This policy identifies specific requirements that must be met by all who use

and/or store sensitive data on electronic devices or electronic media, regardless of whether such media are owned by the University or the individual. This policy does not supplant any other policies, legal requirements, or contractual obligations.

Authorized Users (see definitions) of ISU's IT system (see definitions) must not retain Private Sensitive Information (see definitions) on non ITS-managed electronic devices or electronic media unless the following three conditions have been met:

- A. The Authorized User must justify in writing to the Dean, Department Chair, or Vice President why having Private Sensitive Information stored locally is absolutely necessary to conduct the business of the institution and to perform his or her official duties; and
- B. The Dean, Department Chair, or Vice President must grant written permission to the Authorized User, with a copy being sent to the departmental System Administrator (see definitions) and to ITS. While permission is not required to retain student grades, letters of recommendation, patentable research findings, etc., that are used regularly in the performance of faculty and staff duties, the Authorized User must exercise the same Reasonable Security Precautions (see definitions) to secure the data as if written permission were required.
- C. The Authorized User must exercise Reasonable Security Precautions to secure the Private Sensitive Information that resides on non ITS-managed electronic devices or electronic media.

Private Sensitive Information transferred electronically, other than via fax, must be conveyed using an encrypted method as defined under Reasonable Security Precautions. When sending Private Sensitive Information by fax it must be clearly marked as confidential. Every effort should be made to ensure that only the intended recipient has access to the faxed information.

III. AUTHORITIES AND RESPONSIBILITIES

The author of this policy is the ISU Department of Information Technology Services (ITS). The ISU Security Working Group, in conjunction with representatives from the ISU Office of the Provost and Vice President for Academic Affairs and the Office of the Vice President for Finance and Administration review all changes and updates. Final approval and execution rests with the President of ISU in consultation with university counsel.

IV. DEFINITIONS

For purposes of this policy governing the use of information technology systems and Private Sensitive Information at ISU the following definitions are applicable.

- A. Authorized Users: Include but are not limited to faculty, staff, students, contractors, and guests that are in good standing with ISU and have a valid account for accessing ISU's IT system.

- B. Confidentiality: The state where information can be viewed only by entities that have been authorized to view it. Such authorization may or may not come from the owner or individual.
- C. Crack, or Crackable (as in passwords): A program for discovering passwords that encrypts strings of characters and compare the encrypted text against a file of encrypted passwords. If the two encrypted strings are the same, the string of characters is a valid password.
- D. Due Process: The procedures and practices established and approved by ISU, including notice and an opportunity to be heard , prior to suspension or removal of user privileges where reasonably practicable, and where not reasonably practicable, or in the event of an emergency, as soon thereafter as may be reasonable under the circumstances.
- E. Information Technology Administrator (ITA): the person or office charged with ensuring proper administration and maintenance of ISU's information technology system. The ITA is appointed by the Office of the President. The ITA position may be filled by, but is not limited to, the Chief Information Officer, the Chief Information Security Officer, Information Technology Services and/or other entities designated by the Office of the President.
- F. ISU's IT system: includes, but is not limited to, information systems, networking and telecommunications systems, data processing hardware and software, data transmission equipment and transmission medium, and data storage devices. It also includes stand-alone systems in use by colleges or departments.
- G. Private Sensitive Information:
 - 1. Personal information that, if compromised, could lead to identity theft. Personal information means the first name or first initial and last name of an individual, in combination with and linked to any one or more of the following data elements about the individual:
 - a. Social security number;
 - b. Driver's license number or state identification card number issued in lieu of a driver's license number;
 - c. Passport number; or
 - d. Financial account number, credit card or debit card number, or financial account access codes.
- H. Privacy: the expectation that activities and information stored on a network will not be known by any other individual or entity on the network without authorization or permission of the owner.
- I. SPAM: Unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Sexually explicit unsolicited e-mail is called "porn spam."

Also includes inappropriate promotional or commercial postings to discussion groups or bulletin boards.

- J. System Administrator: an individual designated by the appropriate dean or director charged with administration of local systems that are attached to ISU's IT system. The ITA is notified of such appointments.

PRESIDENTIAL CERTIFICATION

Approved: *Arthur C. Vailas*
President, Idaho State University

Date: *June 26, 2009*