

932 DATA SECURITY POLICY

Policy 932 was approved by the ISU Board of Trustees on July 18, 2003.

932.1 Security of Data. Federal and state laws with regard to privacy and security have become increasingly complex. A network of overlapping federal and state law places a fiduciary obligation on the University to protect the privacy, use, and security of select data. Laws include, but are not limited to: Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), etc. This policy is intended to define the limits of that obligation and the duties and responsibilities of University employees to safeguard information that constitutes protected data.

932.1.1 Scope. Data is considered to be a University resource and as such, policies controlling the collection, use, and dissemination of data are set by the University. ISU employees are expected to know the policies pertaining to data and to abide by their provisions. Access to data by ISU personnel is granted on a need to know basis consistent with their job function.

932.1.2 Definition of Data. Data means numerical or other information represented in a form suitable for processing by computer; factual information, especially information organized for analysis or used to reason or make decisions. For purposes of this policy, data is intended to be defined broadly and is understood to mean all information collected by Indiana State University in the conduct of its business as an educational institution, and any information stored on Indiana State University servers/workstations, or distributed using the ISU network.

932.1.3 Data Classifications. The following definitions shall be used to classify data at ISU.

932.1.3.1 Public Open Access Data. Data that is not personal in nature that requires minimal protection. Threats to data are minimal, and only minimal precautions to protect the data need to be taken. Alteration or destruction of the data is the primary concern.

932.1.3.2 Public Limited Access Data. Data that has limits on access either by contractual arrangements or by the nature of the data. Access is usually restricted to ISU staff and student use. Unauthorized access, alteration, or destruction of the data is the primary concern.

932.1.3.3 Private Releasable Data. Data that is personal in nature but that has been designated as public information (examples are first and last name). Some data in this category can be designated as private by the individual (example is unlisted phone number). Such designation must be in writing – data so designated will be considered “private sensitive data”. Alteration or destruction of the data is the primary concern.

- 932.1.3.4 Private Non-Sensitive Data.** Data whose disclosure would not involve issues of personal credibility, reputation, or other issues of personal privacy and where release of the data is not an overriding concern (example is change of major). Unauthorized access, alteration, or destruction of the data is the primary concern.
- 932.1.3.5 Private Sensitive Data.** Data whose disclosure involves issues of personal credibility, reputation, or other issues of personal privacy protected by law (examples are Social Security number, birthday, and student grades). Data in this classification is often mandated by law but can be so designated by the trustee office responsible for the data. Unauthorized access, alteration, or destruction of the data is the primary concern.
- 932.1.3.6 Restricted/Critical Data.** Data of a sensitive nature that requires a high degree of protection (example is credit card information). Unauthorized access, alteration, or destruction of the data is the primary concern.

932.1.4 Handling of Data.

- 932.1.4.1 Public Open Access Data.** Data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods. Data can be transferred to other non-University owned machines and can be widely distributed.
- 932.1.4.2 Public Limited Access Data.** Data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods. Data can be transferred to other non-University owned machines but can't be shared outside of ISU.
- 932.1.4.3 Private Releasable Data.** Data can be stored and disseminated using minimal protection. Data can be transported using non-secure methods and can be shared outside of ISU on a business need basis.
- 932.1.4.4 Private Non-sensitive Data.** Data can be stored and disseminated using minimal protection. Access is limited on a need to know basis. Data can be transported using non-secure methods. Unless specified to the contrary, data defaults to this category. Data can be transported using non-secure methods and can be shared outside of ISU on a business need basis.
- 932.1.4.5 Private Sensitive Data.** Data is limited on a need to know basis. Data must be kept on centrally supported servers and may be stored in encrypted form. Data may be stored on workstations as needed for short periods of time necessary for processing but must be encrypted and protected from unauthorized access. Access to data is controlled

centrally by a user ID and password. All data being distributed over the network must be encrypted. Hardcopy containing data must be shredded when no longer needed for the intended purpose.

932.1.4.6 Restricted/Critical Data. Data is highly controlled and accessible on a strict need to know basis. Data storage is restricted to servers only and no data will be moved to a workstation for storage. Data must be stored encrypted on central servers that provide both network security (i.e. behind firewall) as well as physical security. Workstations that have access to the data must be located in a physically secured area (locked room/limited access); all write-able media devices removed (i.e. diskette drives, etc.); no software except that required to perform the designated work function is permitted and the workstation must not be connected to the Internet. Data must be encrypted at all times and hardcopy containing restricted/critical data must be shredded when no longer being used.

932.2 Control of Data Access.

932.2.1 Username (ID) and Passwords. Access to controlled data shall be accomplished through the use of usernames (ID) and passwords. (Please see “934 Use of Passwords Policy” for further details.)

932.2.1.1 Access. Access to controlled data (like IDs and passwords) are not to be shared with other employees. As noted above, data dissemination is driven by 1) the classification of the data, and 2) the need to know.

932.2.1.2 Supervision of Students. Student IDs that access ISU data other than public data will be supervised by full-time ISU personnel; the use of the student ID shall be the responsibility of the full-time employee.

932.2.2 Responsibility for Data. Classification and access to controlled data shall be the responsibility of the office designated as the trustee for the respective data (for example, Human Resources would be the trustee for employee data). Disagreements on data classification and access will be resolved by the Chief Information Officer (CIO).

932.2.3 Encryption. Data requiring encryption will be protected by a generally recognized encryption scheme (examples are PGP, Excel encryption, etc.) – use includes digital signatures for email and encryption of stored data.

932.2.4 Employment Policies. Employment policies and procedures relating to compliance with data security policies will be developed by Human Resources.

932.3 No Exceptions. There are no exceptions to this Security of Data Policy.

Last revised February 1, 2011.