

Data Classified as Critical at IU Storage Standard

- Standard - SBIT-101
- Status - Adopted August 1, 2010 - Updated June 18, 2015
- Source - IU South Bend University Information Technology Services (UITS)

Scope

This Standard applies to all users of Indiana University South Bend (IU South Bend) University Information Technology Services resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Rationale

The use of information technologies has become critical in support of most if not all Indiana University operations. This dependence has resulted in a very large, very diverse, and very complex technology environment. At the same time, much more data are being stored, accessed, and manipulated electronically, which has resulted in an increased risk of unauthorized disclosure or modification of personal, proprietary, sensitive, or institutional data. It is very important that everyone associated with providing and using these technology services is diligent in their handling of sensitive data and executing due diligence to assure data integrity.

Standard Statement

IU South Bend organizational units (departments, offices, affiliated agencies, etc.) operating technology resources are responsible for ensuring that data classified as Critical at IU are secured to the level set forth by this Standard. <http://datamgmt.iu.edu/classifications.shtml>

The collection of and storing of data classified as Critical at IU are restricted to legitimate business need such as instances where an outside or government agency requires use of the data, where the data can not be derived from IU central IT systems, when collected during the course of a criminal investigation, or is generated as required during the practice of physical, dental or mental health.

In these cases, and for data classified as Critical at IU not kept in a database, the following Standards apply:

1.
 1. Data classified as Critical should only be stored on systems approved by the University Data Stewards and after consultation with IU South Bend UITS.
 2. The data is to be encrypted using an encryption technology approved by the IU South Bend UITS.
 3. Any transmission of data classified as Critical at IU is to be encrypted.
 4. Data classified as Critical at IU are not to be stored on removable storage media, on personal network drive space (ie...O:), or on a user's personal computer or University issued computer.
- 2.

Procedures

Identifying and Securing data classified as Critical at IU

1. It is the responsibility of the data user to determine if their data is the type of data classified as Critical at IU. Use of scanning tools is recommended to help find certain types of data classified as Critical at IU such as social security numbers or credit card numbers.

2. To determine if the keeping of data classified as Critical at IU are appropriate, consultation with the IU South Bend UITs is recommended.
3. Once the need for keeping data classified as Critical at IU are established, IU South Bend UITs is to be notified to assist with implementing appropriate encryption/logging technology.

Definitions

Database

is a collection of data that is organized so that its contents can easily be accessed, managed, and updated. Typically, the term database refers to the use of special software which organizes data in a specific, and often proprietary format.

Data Owner

is the individual(s) that can authorize or deny access to certain data, and is responsible for its creation, accuracy, integrity, and timeliness.

Encryption Technology

is the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key. Encryption Technology includes that which encrypts data at rest and in transit.

Network Storage

is the data storage location managed by Information Technologies and is commonly referred to as having a drive letter H:, or is storage location setup specifically for a special type of system, such as software which utilizes database technology.

Removable Storage Media

includes all types of devices which store data, such as flash drives, Optical Discs (CD, Blue-Ray or DVD), MP3 players, Memory cards (CompactFlash card, Secure Digital card, Memory Stick), PDAs, externally connected hard drives, floppy disks, electromagnetic tape, or the like.

Data Classified as Critical at IU

refers to any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on University interest or the privacy to which individuals are entitled. Examples of data classified as Critical at IU include social security numbers, credit card numbers, medical or mental health records, certain forms of professional/client privilege, and certain types of institutional data.

Sanctions

Failure to comply with Indiana University South Bend information technology standards and policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); to the individual's employment (up to and including immediate termination of employment); civil or criminal liability; or any combination of these.

Related Policies, Laws, and Documents

- [IT-07 Privacy of Information Technology Resources](#)
- [IT-12 Security of Information Technology Resources](#)
- [SBIT-102 Electronic Media Disposal/Redistribution Standard](#)
- HIPAA Regulations
- PCI-DSS Standards
- FERPA Regulations

Campuses, schools, colleges, departments, and other administrative units may have issued local policies and standards governing the appropriate use of information technologies deployed specifically to support that unit's activities. Managers of information technology services may have issued service-level policies and standards governing the appropriate use of their services. In order to understand and adhere to these requirements, users of these resources are responsible for consulting with appropriate unit or service staff.

Consultation:

IU South Bend UITS is available to provide consultation or advice related to technology use or misuse to any university, campus, or unit administrators or individual personnel.

Standard History

- [Approved August 1, 2010](#)
- Updated June 18, 2015 - new wording to reflect UITS reorganization