

Data Security Policy

Introduction

Institutional data is information that supports the mission and operation of Tennessee Tech University. It is a vital asset and is owned by the University. Some institutional data may be distributed across multiple departments or units of the University, as well as outside entities. Institutional data is considered essential, and must comply with legal, regulatory, and administrative requirements.

Departments and units must assess institutional risks and threats to the data for which they are responsible, and accordingly classify its relative sensitivity as Level I (low sensitivity), Level II (moderate sensitivity), or Level III (high sensitivity). *Unless otherwise classified, institutional data is Level II.* University personnel may not broaden access to institutional data without authorization from the department or unit responsible for the data. This limitation applies to all means of copying, replicating, or otherwise propagating university data.

All data shares to be set up between systems must be requested via ITS to ensure data integrity.

Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality (need for secrecy), but also the need for integrity and availability. The need for integrity, or trustworthiness, of institutional data should be considered and aligned with institutional risk; that is, what is the impact on the institution should the data not be trustworthy? Finally, the need for availability relates to the impact on the institution's ability to function should the data not be available for some period of time. There are three classification levels of relative sensitivity which apply to institutional data:

Level I: Low Sensitivity

Access to Level I institutional data may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of "Public" data should be protected, and the appropriate department or unit must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level I data not be available is typically low, (inconvenient but not debilitating). Examples of

Level I "Public" data include published "white pages" directory information, maps, departmental websites, and academic course descriptions.

Level II: Moderate Sensitivity

Access to Level II institutional data must be requested from, and authorized by, the department or unit who is responsible for the data. Access to internal data may be authorized to individuals based on job classification or responsibilities ("role-based" access), and may also be limited by one's employing unit or affiliation. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the institution should this information not be available when needed is typically moderate. Examples of Level II "Non-Public/Internal" institutional data include project information, official university records such as financial reports, human resources information, some research data, unofficial student records (including grade books without SSNs), and budget information.

Level III: High Sensitivity

Access to Level III institutional data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted data must be individually requested and then authorized by the department or unit who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Level III "Confidential/Restricted" data include official student grades and financial aid data; social security and credit card numbers; individuals' health information, and human subjects research data that identifies an individual.

Policy Statement

- Institutional data must be protected from unauthorized modification, destruction, or disclosure. Permission to access institutional data will be granted to all eligible University employees for legitimate university purposes.
- Authorization for access to Level II and Level III institutional data comes from the department or unit, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other authority.
- Where access to Level II and Level III institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.

- University employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction in accordance with TBR Guideline B-080.
- Departments and units must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with University policy and procedure.
- Departments and units must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Data Handling Requirements

	LEVEL I Low Sensitivity (Public Data)	LEVEL II Moderate Sensitivity (Non-Public/ Internal Data)	LEVEL III High Sensitivity (Confidential/ Restricted Data)
Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; no labels required	Must be sent via Confidential envelope; reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	As authorized by department or unit	As authorized by department or unit	Prohibited
Information stored on CD/DVD, tape, floppy, or other archival media	See Physical Access controls	See Physical Access controls	Encryption via approved method or Physical Access controls
Physical Access Controls (CD/DVD, tape, floppies, paper, or other archival media)	No special controls	Access-controlled area	Access-controlled and monitored area with restricted access or vault; paper archives must be in locked storage facilities with limited key distribution or in locked filing cabinets

External Data Sharing	No special controls	As allowed by TN Law	As allowed by Federal regulations; TN Law; FERPA restrictions
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmission
Data Tracking	None	None	Social Security Numbers, Credit Cards, and PHI locations must be registered with the appropriate campus entity
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destruction of electronic media
Auditing	No controls	Changes	Logins, accesses and changes
Information stored on workstations and mobile devices	Password protection recommended	Password protected	Password protected; encryption via approved encryption method
Physical Access Controls (workstations, laptops, USB flash drives, servers, PDAs, and cell phones)	Locked when not in use	Access-controlled area; locked when not in use	Access-controlled and monitored area; locked when not in use

Control Definitions

Mailing & Labels on Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.

Electronic Access – How authorizations to information in each classification are granted.

Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.

Physical Access Controls – The protections required for storage of physical media that contains the information. This includes, but is not limited to workstations, servers, CD/DVD, tape, USB flash drives, floppies, cell phones, paper, laptops, and PDA's.

External Data Sharing – Restrictions on appropriate sharing of the information outside of TTU

Electronic Communication – Requirements for the protection of data as transmitted over telecommunications networks.

Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations to the appropriate university entity.

Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus), as outlined in other key policies.

Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them.

Information stored on workstations and mobile devices – Requirements for the protection of information stored locally on workstations and mobile devices. This includes, but is not limited to laptops, tablet computers, PDAs, cell phones, and USB flash drives.

Each employee must confirm their understanding of and agreement with this Data Security policy by signing the Confidentiality Agreement located at <http://www.tntech.edu/its/policies>

For information regarding the approved/recommended encryption devices and methods, please see:

http://www.tntech.edu/its/news/Security_Tips/EncryptionMethods.htm

Revision 1.3 recommended by the Information Technology Committee 02/28/08