ITS POLICIES AND GUIDELINES
CATEGORY: Information Technology, Security, Privacy, Information Access & Management
STATUS: In Review

POLICY TITLE: **Data Security Policy**

POLICY PURPOSE:
This policy serves to outline essential roles and responsibilities within the University community for creating, accessing, transmitting, and storing University data, to identify procedures that should be put in place to protect the confidentiality, integrity and availability of University data, and to comply with legal, regulatory, and University policy and procedures regarding use, privacy and confidentiality of information.

University data is any data that is owned or licensed by the University and includes any data related to Truman State University (University) functions that are: a) stored on University information systems, b) maintained by University faculty, staff, or students, or c) related to institutional processes on and off campus. This applies to any format or media (meaning it is not limited to electronic data). Determining how to protect and handle information depends on a consideration of the information's type, importance, sensitivity, and usage.

Classification is necessary to understand which security practices should be used to protect different types of data. Classification is according to the risks associated with data being stored or processed. Data with the highest risks need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Four levels of data classification will be used to classify University data: Level I (Confidential Information), Level II (Sensitive Information), Level III (Public Information), and Level IV (Proprietary Information).

APPLIES TO:
- All members of the Truman State University community
- Anyone granted access to Truman State University data, systems or networks

---

Contents:

POLICY STATEMENT:

Responsibility for Data Management
Data is a critical asset of the University. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of any data that is created, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of the format (such as electronic, paper or other physical form).

Campus units are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of University data in compliance with this policy and for carefully evaluating the appropriate data classification category for their information.

- University data must be protected from unauthorized modification, destruction, or disclosure. Permission to access University data will be granted to all eligible University employees for legitimate university purposes.
- Requests for access to Level I and Level II University 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 I and Level II University 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 University data is at risk of unauthorized access, modification, transmission, storage, disclosure, or destruction. To report these instances, contact the Information Technology Services Office at (660) 785-4163.
- Departments and units must ensure that all decisions regarding the collection and use of University data are in compliance with legal, regulatory, and University policy and procedures regarding use.
- Departments and units must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect University data.
- Authorized 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, regulations, and policies with respect to accessing, using, or disclosing information.
- Any Information System that stores, processes, or transmits University data shall be secured in a manner that is considered reasonable and appropriate, given the level of sensitivity, value and criticality.

Data Classification
Determining the classification level of University data should be done according to an assessment of the need for confidentiality of the information, a consideration of the University data based on how the data is used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies. The classification of the most sensitive element in a data collection will determine the data classification of the entire collection. University data classifications are as follows:

Level I – Confidential Information
Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Custodian/Owner is required for access because of legal, contractual, privacy, or other constraints. This classification has a high risk of significant financial loss, legal liability, public distrust, or harm if data is disclosed.

Examples include:

Personally Identifiable Employee Information - Personally identifiable employee information is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Employer identification number (Banner ID)
- Social Security Number
- Passport number
- Personnel records as defined in the Truman Records Management Procedures

Information is considered personally identifiable if it can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Personally Identifiable Education Records – covered under the Federal Educational Rights and Privacy Act (FERPA) – Personally identifiable education records are defined as education information in combination with one or more of the following data elements:

- Student identification number (Banner ID)

- Student Name (a person's first name or first initial and last name)
- Social Security Number
- Passport number
- Race/Gender

Information is considered personally identifiable if it can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Personally Identifiable Financial Information (PIFI) – covered under Gramm-Leach-Bliley Act (GLBA) - For the purpose of meeting security breach notification requirements, PIFI is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

Information is considered personally identifiable if it can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Protected Health Information (PHI) – covered under the Health Insurance Portability and Accountability Act (HIPAA) - PHI is defined as any individually identifiable information that is stored by a Covered Entity [1], and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual.

Information is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone/FAX numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- University Resource Locators (urls)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe the information can be used to identify an individual, it is not considered "individually identifiable" and, as a result, would not be considered PHI.

[1] The term "covered entity" under the HIPAA Privacy Rule refers to three specific groups, including health plans, health care clearinghouses, and health care providers that transmit health information electronically.

Payment Card Information – covered under the Payment Card Industry Data Security Standards (PCI DSS) **-** Payment card information is defined as the credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Credit card number (in part or whole)[2]
- Primary Account Number (PAN)
- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2, or CID value (values unique to each credit card and used as secondary card validation)
- PIN or PIN block
- Contents of a credit card's magnetic stripe

[2] Truman does not store credit card numbers in any of its systems. Credit card processing, along with all eCommerce processing, is handled through contracted remote services.

Level II – Sensitive Information

Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. This classification has a moderate requirement for confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.

Examples include:

- Financial accounting data that does not include confidential information
- Departmental intranet
- Directory information for students, faculty, and staff who have requested nondisclosure (for example, per FERPA for students)
- Some research data
- Budget information

Level III – Public Information

Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the University, affiliates, or individuals. This classification has a low requirement for confidentiality and/or low or insignificant risk of financial loss, legal liability, public distrust, or harm if the data is disclosed.

Examples include:

- Truman public web site
- Directory information for students, faculty, and staff except for those who have requested "Directory Restriction" (for example, per FERPA for students)
- Course descriptions
- Semester course schedules
- Press releases
- Departmental websites

Level IV – Proprietary Information

Data provided to or created and maintained by Truman State University on behalf of a third party, such as a corporation or government agency, will vary in its handling requirements depending on contractual agreements and/or relevant laws or regulations. The classification and security standards for proprietary data owned by the third party will be defined by the third party. Proprietary data owned by Truman State University must be classified and protected according to Truman's data classification policy and security standards. Individuals managing or accessing proprietary data are responsible for complying with any additional requirements and security policies

and procedures specified by the third party owner. This classification ranges from high to low risk depending on the terms of the contractual agreements and the content of the data.
Examples include:

- Financial sponsored program data
- Data maintained by certain researchers who have special data arrangements with public or personal agencies
- Data maintained by commercial account owners

All information should be categorized and protected according to the requirements for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.

- Data custodians/owners must determine the data classification of the University data that is their responsibility and must ensure that it is protected in a manner appropriate to its classification.
- No University-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- High risk, confidential data must be encrypted during transmission over insecure channels.
- Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.
- Any data covered by federal or state laws or regulations or contractual agreements must meet the security and use requirements defined by those laws, regulations, or contracts.

Contracts with Third Parties
Contracts between the University and third parties involving University data must include language requiring compliance with all applicable laws, regulations, and University policies related to data and information security; immediate notification of the University if University data is used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure.

Data Handling 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.
- *Secondary Use* – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application/project.
- *Electronic Access Authorization* – How authorizations to information in each classification are granted. Role-based access is an access role defined that includes one or more individuals having that role assigned to their accesses and the access grants them the ability to query or update data such as create requisitions. Examples: Level I data cannot be stored on departmental W: drives as role-based access is defined for W: drives (meaning all departmental staff have access to the departments W: drive). Y: drives are individually authorized storage.
- *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/smart phones, paper, laptops, and PDA's.

- *External Data Sharing* – Restrictions on appropriate sharing of the information outside of Truman State University.
- *Electronic Communication* – Requirements for the protection of data as transmitted over telecommunication networks. Transmission includes all transfer protocols including sftp, scp, and email. Example: Level I data could not be emailed unless it was encrypted and it is recommended to encrypt Level II data before it is emailed especially to external sources.
- *Data Disposal* – Requirements for the proper destruction or erasure of information when the storage devise it resides on is decommissioned (transfer or surplus), as outlined in other key policies. This also includes when the storage device is to be repurposed and includes internal, external, and removable media. For paper reports shredding with a cross-cut shredder is recommended for Level II data and required for Level I data.

Data Handling Requirements

	Level I – Confidential	**Level II – Sensitive**	**Level III – Public**
Mailing & Labels on Printed Reports	Must be sent via Confidential envelope; reports must be marked "Confidential"	May be sent via Campus Mail; no labels required	None
Secondary Use	Prohibited	As authorized by department or unit	As authorized by department or unit
Electronic Access Authorization	Individually authorized, with a confidentiality agreement	Role-based authorization	No controls
Physical Access Controls	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	Access-controlled areas	No special controls
External Data Sharing	As allowed by regulatory, legal, and policy restrictions	As allowed by legal, regulatory, and policy restrictions	No special controls
Electronic Communication	Encryption required for all transmission	Encryption recommended for external transmission	No special controls
Data Disposal	Shred reports; Department of Defense-Level wipe or destruction of electronic media	Shred reports; Wipe/erase media	None

Note: Level IV – Proprietary Data handling requirements will be based on the definition of each set of data and any additional requirements that may be included in the contractual agreements associated with the data/project.

Routine Data Handling
Routine data handling procedures and more specific details for data handling can be found in the Data Handling Procedures Guidelines.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:
Any exceptions to this policy must be approved in writing by ITS (see contact information below).

CONSEQUENCES:
Individuals failing to abide by this policy or policy procedures may be subject to sanctions up to and including the loss of computer or network privileges, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

CONTACTS:

Responsible Executive:	Provost and Vice President for Academic Affairs
Responsible Office:	Information Technology Services
Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	Truman State University President
APPROVED ON:	March 1, 2012
EFFECTIVE ON:	March 1, 2012
REVIEW/CHANGE HISTORY:	
REVIEW CYCLE:	Annual

DEFINITIONS:

Authentication is the process of verifying one's digital identity. For example, when someone logs onto a computer, the password verifies that the person logging in is the owner for the account. The verification process is called authentication.

Authorization is granting access to resources only to those authorized to use them.

Authorized users are (1) current faculty, staff, students, and affiliates of the University and (2) others whose temporary access furthers the mission of the University. Authorized users gain access to University resources through the hiring process, the student admissions process, designation as a University "affiliate", or as a guest or vendor upon approval by a University administrator.

Confidentiality preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data Custodians/Owners support the mission of the University and facilitate the conduct of University business by ensuring that access to data is granted as needed for legitimate purposes and within the terms articulated in these and other University policies. For University data that sources from the Banner Administrative System, Data Custodians have been identified in the Data Standards Document.

Department includes academic and administrative organizational entities at Truman.

Directory Restriction is the coding placed on an individual's record when they request that their directory information be withheld from release. Students may have this restriction established by contracting the Registrar.

External agencies are entities such as customers, partners, government and/or state regulators, and the society, which interact with the University and may influence its performance, but are not under its direct control.

General user-level passwords are for day to day use of the University information technology resources. These accounts will not have system level privileges with the exception of authorized users that have administrative privileges on their own workstations.

Information System is defined as any electronic system that stores, processes, or transmits information.

ITS – Information Technology Services

Primary Account Number (PAN), also referred to as "account number", is the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Note: Truman does not store credit card numbers in any of its systems.

Removable Media are data storage media including but not limited to magnetic tape, diskettes, zip disks, removable disk storage, USB drives, and CD/DVDs that can be removed from a Computer System and easily carried from place to place.

Sensitive Information is information maintained by the University which requires special precautions to ensure its accuracy and integrity. It is information that requires a high level of assurance of accuracy and completeness.

University is used interchangeably with Truman State University.

University affiliates are the people and organizations associated with the University through some form of formalized agreement.

University data is defined as any data that is owned or licensed by the University and may include any data related to Truman State University (University) functions that are: a) stored on University information systems, b) maintained by University faculty, staff, or students, or c) related to institutional processes on and off campus. This applies to any format or media (meaning it is not limited to electronic data).

RELATED DOCUMENTS:

Data Standards Document (http://its.truman.edu/admincomputing/Data%20Standards_Truman.v.3.0.pdf)
Data Handling Procedures Guidelines
Family Educational Rights and Privacy Act of 1974 (FERPA - http://fedinfo.truman.edu/ferpa.asp)
Health Insurance Portability and Accountability Act of 1996 (HIPAA – http://www.hhs.gov/ocr/privacy)
Payment Card Industry Data Security Standard (PCI DSS - https://www.pcisecuritystandards.org/security_standards/index.php)
Missouri Sunshine Law (Open records - http://ago.mo.gov/sunshinelaw/sunshinelaw.htm)
Truman Records Management Procedures

KEYWORDS: