The University of Texas Rio Grande Valley
Information Security Office

Minimum Security Standards for Data Stewardship

Table of Contents

1. Purpose

This minimum standard serves as a supplement to the Information Resources Use and Security Policy, which was drafted in response to Texas Administrative Code 202 and UT System UTS-165. Adherence to the standard will improve confidentiality and integrity of university data.

The objective of this standard is to facilitate the identification, management, communications and training requirements to promote prudent stewardship of university data. This minimum standard exists in addition to all other university policies and federal and state regulations governing the protection of the university's data.

Compliance with these requirements does not imply that data will be completely secure. Instead, these requirements should be integrated into a comprehensive information security plan.

2. Scope

This standard applies to the handling of university data that are classified as Confidential, Controlled, or Published (see Data Classification Standard).

3. Audience

All faculty, staff, student employees, contractors, and vendors working with University of Texas Rio Grande Valley data or information resources.

4. Minimum Standard

The university requires all data stewards and data custodians to manage, access, and utilize university data in a manner consistent with the university's need for confidentiality, integrity, and availability.

Each College, School, or Unit (CSU) handling university data shall develop, maintain, and execute a data stewardship plan comprised of clear and consistent procedures describing how the respective area manages the handling, access, and protection of university data. Each data stewardship plan for university data shall include the following components:

4.1. General identification of all Confidential data handled and retained by the CSU.

4.2. Specific procedures addressing the handling of printed data, including but not limited to:

4.2				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.2.1	Labeling documents	Certain documents must be labeled as "Confidential" regardless of internal or external use. Documents approved for distribution should be labeled accordingly.	Certain documents may be labeled as "Confidential" regardless of internal or external use. Documents approved for distribution should be labeled accordingly.	No special requirement
4.2.2	Duplicating documents	Receiver of document containing Confidential information must not further distribute without permission of respective CSU or data steward. Please see records management practices for more details about creating and managing copies of records.	No special requirement	No special requirement
4.2.3	Mailing documents via campus mail	The envelope is labeled as "Confidential"	No special requirement	No special requirement
4.2.4	Mailing documents via external mail carriers	No classification marking on external envelope required; Confirmation of receipt is required as legally mandated.	No special requirement	No special requirement
4.2.5	Disposing of documents	Adhere to retention schedules. Employ the services of the preferred vendor for records management and destruction.	Adhere to retention schedules. Physical destruction beyond ability to recover (e.g. office cross-cut shredder).	Refer to retention schedules. No special requirement.

4.2				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.2.6	Storing of documents	Stored in a secured location when not in use.	Stored out of sight when not in use.	No special requirement
4.2.7	Granting permission to view information	Read access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	Read access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	No special requirement
4.2.8	Reviewing data classifications for data under CSU and Data Stewards' management	Review annually	Review annually	Review annually

4.3. Specific procedures addressing the storage of digital data, including but not limited to:

4.3				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.3.1	Storing data on fixed media with access controls.	No encryption required. It is highly recommended that some credit card and/or bank account information be encrypted if it must be stored. (Refer to the Data Encryption Guidelines for information about encryption.) Sensitive credit card authentication data should not be stored at all.	No special requirement	No special requirement
4.3.2	Storing data on fixed media without access controls and accessible via the network	Not permitted.	Not advised. If Controlled data must be stored via this media, it should be encrypted (see Data Encryption Guidelines) or isolated in such a manner that ensures confidentiality, integrity, and/or availability.	No special requirement
4.3.3	Storing data on fixed media without access controls, but not accessible via the network	Devices must be stored in a physically secured location at all times.	Devices must be stored in a physically secured location when not in use.	No special requirement

4.3				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.3.4	Storing data on removable media or portable devices	It is required that Confidential data be encrypted when stored on such media or devices (see Information Acceptable Use and Security Policy (AUP)). Such media or devices must be stored in secured location when not in use.	It is recommended that Controlled data be encrypted when stored on such media or devices. Such media or devices must be stored in secured location when not in use.	No special requirement
4.3.5	Granting permission to view data (including duplication)	Read access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	Read access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	No special requirement
4.3.6	Granting permission to create or modify data	Create / Modify access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	Create / Modify access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Steward, or their designate.	No special requirement
4.3.7	Granting permission to delete data	Deletions are restricted using various access control methods and are based on roles, classes, entitlements, or affiliations defined by respective Data Steward or their designate. Also adhere to records management requirements for deleting data.	Deletions are restricted using various access control methods and are based on roles, classes, entitlements, or affiliations defined by respective Data Steward or their designate.	No special requirement

4.3				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.3.8	Preventing data disclosure to unauthorized requestors (e.g., social engineering)	Consider what is being requested and who is requesting it. If the requestor's credentials or authenticity cannot be 100% assured, do not disclose any information. Escalate the situation to a supervisor, or to the Information Security Office.	Consider what is being requested and who is requesting it. If the requestor's credentials or authenticity cannot be 100% assured, do not disclose any information. Escalate the situation to a supervisor, or to the Information Security Office.	No special requirement
4.3.9	Preventing unauthorized viewing or eavesdropping of data (e.g., shoulder surfing)	Implement privacy screens on monitors that are in high-traffic areas. Be aware of any unauthorized individuals or loiterers.	Implement privacy screens on monitors that are in high-traffic areas. Be aware of any unauthorized individuals or loiterers.	No special requirement
4.3.10	Printing hard copy report of data	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing.	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing.	No special requirement
4.3.11	Labeling data at the internal application or screen level	If information has been specifically restricted (e.g. about a user), it should be clearly displayed to the viewer upon request of such restricted information.	No special requirement	No special requirement
4.3.12	Disposing of surplus physical electronic media device (e.g. disks, hard drives, CDs, etc)	Media must be securely destroyed using university-approved methods.	Media should be wiped or degaussed beyond the ability to recover data. It is advised that media be destroyed using the	No special requirement

4.3				
#	**Action**	**Confidential**	**Controlled**	**Published**
			Confidential destruction processes	
4.3.13	Disposing of data (e.g., legacy data, unneeded data, etc)	Adhere to retention schedules. Manually or automatically attempt to verify Confidential data has been removed (e.g., identity finder).	Adhere to retention schedules. Manually or automatically attempt to verify Controlled data has been removed.	No special requirement
4.3.14	Auditing access activity	Log all necessary access attempts defined by policy or business requirements; System Custodians shall review all access violation attempts and notify Data Steward and/or Information Security Office of any suspicious or abnormal activity.	Log all violation attempts; System Custodian reviews as appropriate.	No special requirement
4.3.15	Retaining information access report logs	Retain logs for at least 14 days. Existing record retention schedules are authoritative.	Retain logs for at least 14 days. Existing record retention schedules are authoritative.	No special requirement
4.3.16	Reviewing data classifications for data under CSU and Data Stewards' management	Review annually	Review annually	Review annually

4.4. Specific procedures addressing the transmission of digital data, including but not limited to:

4.4				
#	**Action**	**Confidential**	**Controlled**	**Published**
4.4.1	Transmitting information via fax	Machine must have limited access such that only those authorized can view. Otherwise, recipient must first agree that an authorized person will be present when the material is received.	Machine must have limited access such that only those authorized can view. Otherwise, recipient must first agree that an authorized person will be present when the material is received.	No special requirement
4.4.2	Transmitting information via voice mail	Confidential data must not be provided in a voice mail message. Instead, request a call back.	No special requirement	No special requirement
4.4.3	Transmitting information via wired, wireless, or cellular network	Encryption required (e.g. SSL, SSH, IPSEC, etc). If no secure transmission option is available, data must be encrypted prior to transmission.	Encryption suggested	No special requirement
4.4.4	Transmitting information via other network protocols (e.g. e-mail, file transfers, telnet sessions, web applications, network printing)	Encryption required (e.g. SSL, SSH, IPSEC, etc). If no secure transmission option is available, data must be encrypted prior to transmission.	Encryption suggested. Access controls required.	No special requirement
4.4.5	Reviewing data classifications for data under CSU and Data Stewards' management	Review annually	Review annually	Review annually

5. Responsibility

5.1. Colleges, Schools, Units (CSUs)

5.1.1. CSUs, relying on the university's Data Classification Standard and the Minimum Security Standards for Data Stewardship, shall develop, maintain, and execute a data stewardship plan comprised of clear and consistent procedures describing how the respective functional areas and their reporting units manage the handling, access, and protection of university data.

5.1.2. CSUs must be able to clearly demonstrate effective employee awareness efforts as they relate to respective business practices involving university data.

5.2. Data Stewards

5.2.1. Data Stewards shall ensure that steps are taken to protect the data in accordance with respective policies, guidelines, and procedures are being properly implemented.

5.2.2. Data Stewards may delegate the implementation of the university polices, guidelines, and procedures (for example, system administration) to professionally trained campus or departmental IT owners and/or custodians.

5.3. Data Custodians

5.3.1. All university employees handling university data are considered Data Custodians for any data in their possession regardless of where the data may be stored.

5.3.2. Data Custodians should review and understand the university's Data Classification Standard and the responsibilities associated with viewing and handling university data they have been authorized to access. Any related questions should be directed to their respective supervisor and/or to the Information Security Office (is@utrgv.edu).

5.3.3. Data Custodians should refer to the Minimum Security Standards for Data Stewardship, or their respective area or unit's specific data handling procedures, if there are any questions about how a piece of data should be handled.

5.3.4. Data Custodians are responsible for any unauthorized disclosure or exposure of data while the data is in their possession.

5.3.5. All university employees handling university data should avoid accessing, manipulating, or changing university data without the authorization of their supervisor or if is not required to fulfill assigned university duties. Such misuse includes, but is not limited to, the following examples:

5.3.5.1. Changing data about yourself or others for other than usual business purposes.

5.3.5.2. Using information, even if authorized to access it, to support actions by which individuals might profit (e.g., salary changes, grade changes, appointment changes.)

5.3.5.3. Disclosing information about individuals without prior supervisor authorization.

5.3.5.4. Monitoring the pattern of salary raises of others; determining the source and/or destination of telephone calls or Internet usage; patterns of personal location; exploring race and ethnicity indicators; querying student grades.

5.3.5.5. Circumventing the assigned levels of data access given to other users by providing access or data sets that are broader than those available via normal approved levels of access.

5.3.5.6. Facilitating another's illegal access to or compromise of the university's information resources by sharing account passwords or other information.

5.3.5.7. Violating university policies or federal, state, or local laws in accessing, manipulating, or disclosing university data.

6. Non-Compliance and Exceptions

For all CSUs and Data Stewards — if any of the minimum standards contained within this document cannot be met with regard to Confidential or Controlled data that you manage or support, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management. (See Security Exception Form.)

For all university employees — non-compliance with this standard may result in revocation of system or network access, notification of supervisors, and/or reporting to the Offices of Internal Audit and Institutional Compliance.

All University of Texas Rio Grande Valley employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas Rio Grande Valley employees are required to comply with federal and state laws and regulations.

7. Related UTRGV Policies, Procedures, Best Practices, and Applicable Laws

The policies and practices listed here inform the system hardening procedures described in this document and with which you should be familiar. (This is not an all-inclusive list of policies and procedures that affect information technology resources.)

UT System (UTS 165) Information Resources Use and Security Policy
UTRGV (AUP) Acceptable Use Policy
Computer Security Standard
Extended list of confidential data
Data Classification Guide
Data Protection Standard for Personally Owned Mobile Devices

8. Sources

UT – Austin Information Security Office
(https://security.utexas.edu/policies/standards_stewardship)

9. Revision History

Revision History			
Version	**Date**	**New**	**Original**
1.0	3/20/2017	Created document	Entire document has changed.

10. Approvals

Approvals		
Name	**Role**	**Date**
Thomas Owen	Approval	4/13/2017