Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

PROTECTION BY DATA CLASSIFICATION SECURITY STANDARD

Security Standards are <u>mandatory</u> security rules applicable to the defined scope with respect to the subject.

Overview

Information must be protected according to its sensitivity, criticality, and value, whether it is printed, stored, or transmitted. All elements of protection need to be taken into consideration, which include but are not limited to: desktops, servers, networking equipment, filing cabinets, fax machines, voice mail, paper, etc. Information resources need protection from unauthorized access, modification, disclosure, or destruction. Data classification with protection requirements communicate the specific expectations.

Scope

All departments, offices, and schools are responsible for UTHSCSA's information resources and must protect information according to its importance. UTHSCSA's data classifications create a framework of information categories for evaluating the information's relative value and defining appropriate controls for protection required by this security standard. When evaluating data that may have overlapping classifications based on data and circumstances, the document should be rated at the higher classification. The data owner, with support from the data custodian, is ultimately responsible for assigning data classifications. This standard applies to all applicable documents and data created or modified after the effective date of this standard. Other documents, data, records, etc., may be classified as time permits.

Purpose

The purpose of this document is to communicate required protection for information resources based on UTHSCSA's Data Classification Policy. It is the responsibility of all UTHSCSA departments, offices, and schools to protect the information based on the requirements outlined in this document. In all cases, reasonable precautions and protections should be taken, regardless of classification.

Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

Protection

	Public	Internal	Confidential	Confidential/High Risk
Definition	Information that is widely available to the public through publications, pamphlets, web content, and other distribution methods	Routine operational information requiring no special measures to protect from unauthorized access, modifications, or disclosure, but not widely available to the public	Confidential or sensitive information that **would not** necessarily, due to Federal or State law, **expose the University to significant loss**, but the data owner has determined security measures are needed to protect from unauthorized access, modifications, or disclosure	Information requiring the highest levels of protection because disclosure is likely to result in **significant adverse impact to the institution** (embarrassment, financial loss, sanctions, penalties, etc.)
Examples	Patient brochures, news releases, pamphlets, web sites, marketing materials	Routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, internal policies & procedures	Intellectual property licensed and/or under development, contract research protocols, records, department financial data, purchasing information, vendor contracts, system configurations, system logs, risk reports	Protected Health Information (PHI), Student Identifiable Information (SII), personnel information, Social Security Numbers; intellectual property licensed and/or under development
Marking				
1. Documents	1. No restrictions	1. Bottom of every page should be labeled “Internal Use Only”, whether stored, printed, or transmitted	1. Top of every page should be labeled “Confidential” whether stored, printed, or transmitted	1. Top and bottom of every page must be marked “Confidential” whether stored, printed, or transmitted
2. Internally-routed envelopes	2. No restrictions	2. No requirements	2. Marked “Confidential”	2. Marked “Confidential”
3. Externally-routed envelopes	3. No restrictions	3. No requirements	3. Contain an internal envelope marked “Confidential”, but the external envelope should not reflect the sensitivity of the information	3. Contain an internal envelope marked “Confidential”, but the external envelope **must** not reflect the sensitivity of the information

Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

	Public	Internal	Confidential	Confidential/High Risk
Release	Available to the general public and for distribution outside of the organization	• Intended for use only within the organization • May be shared outside the organization only if there is a legitimate business need to know, and is approved by management	• Access limited to a need-to-know basis and not to be released externally, unless in accordance with specified policies and procedures on release of information • When releasing information, sensitivity and protection requirements must be communicated • Controls must be in place to prevent unauthorized copying or use of intellectual property	• Access limited to **as few persons as possible** on a need-to-know basis and not to be released externally, unless in accordance with specified policies and procedures on release of information • When releasing information, sensitivity and protection requirements must be communicated • Controls must be in place to prevent unauthorized copying or use of intellectual property • **Information is very sensitive and must be closely controlled from creation to destruction**
Transmission by Spoken Word Examples include conversations, meetings, telephones, cellular phones, voicemail, and answering machines	No special precautions required	Reasonable precautions to prevent inadvertent disclosure	Active measures to prevent unauthorized parties from overhearing information • Discuss in private setting with lowered voices • Avoid conversations in public areas, e.g. elevators, hallways, cafeterias, etc. • Avoid proximity to unauthorized listeners • Use speaker phone in secure area only • Use of cellular telephones discouraged, wired line preferred • No public announcements • Initiate calls or positively identify the person you are speaking with	Active measures and close control to limit information to as few persons as possible • **Discuss in enclosed meeting areas only** • **Discussions in public areas prohibited** • Avoid proximity to unauthorized listeners • Use speaker phone in enclosed secure area only, **though use is generally discouraged** • Use of cellular telephones discouraged, wired line preferred • No public announcements • Initiate calls or positively identify the person you are speaking with

Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

	Public	Internal	Confidential	Confidential/High Risk
Transmission by Post				
1. Mail within the organization (interoffice)	1. Ensure appropriate routing information is used (name, address, etc.)	1. Ensure appropriate routing information is used (name, address, etc.)	1. Sealed inter-office envelope marked "Confidential". Ensure appropriate routing information is used (name, address, etc.)	1. Sealed inter-office envelope marked "Confidential**". Notify recipient in advance**. Ensure appropriate routing information is used (name, address, etc.)
2. Mail outside of the organization	2. Ensure appropriate routing information is used (name, address, etc.)	2. Ensure appropriate routing information is used (name, address, etc.)	2. 1st class mail (minimum requirement). Trackable delivery preferred, e.g. messenger, FedEx,U.S. express or certified, return receipt mail. Ensure appropriate routing information is used (name, address, etc.)	2. **Trackable delivery required,** e.g., messenger, FedEx, DHL, U.S. express or certified, return receipt mail. Ensure appropriate routing information is used (name, address, etc.)
Transmission by facsimile (fax)				
1. Location of fax	1. No special restrictions	1. Located in area not accessible to general public	1. Located in area not accessible to general public	1. Located in area not accessible to general public **and/or unauthorized persons**
2. Handling procedures	2. Reasonable care in dialing	2. Reasonable care in dialing	2. Required Handling: • Cover sheet labeled "Confidential" • Procedures to validate transmission to intended recipient, e.g. validated direct dial key, confirmation print out • Ensure remote fax machine is being monitored by authorized recipient • Removal of received fax immediately • If automated, similar controls should be implemented.	2. Required Handling • Coversheet labeled "Confidential" • **Preferred telephone notification prior to transmission and subsequent telephone confirmation of receipt required** • Ensure remote fax machine is being monitored by authorized recipient • Removal of received fax immediately • If automated, similar controls must be implemented

Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

	Public	Internal	Confidential	Confidential/High Risk
Transmission to Printer				
1. Location of Printer	1. No special restrictions	1. Located in area not accessible to general public	1. Located in area not accessible to general public	1. Located in area not accessible to general public **and/or unauthorized persons**
2. Handling	2. No special restrictions	2. Reasonable care in validating printer location	2. Required Handling: • Ensure device is being monitored by authorized individual • Removal of printed material immediately	2. Required Handling: • Ensure device is being monitored by authorized individual • Removal of printed material immediately
Transmissions Internally				
1. E-mail within the organization	1. No special handling required	1. No special handling required, but reasonable precautions should be taken	1. Use of e-mail to transfer confidential information is discouraged. Forwarding only allowed by data owner	1. Use of e-mail to transfer confidential information is discouraged. . Forwarding only allowed by data owner
Transmissions Externally (IM, email, Chat, file transmission, etc.)				
1. Data transfers (file transmissions, website, etc.)	1. No special precautions are required	1. Encryption is recommended but not required	1. Encryption is required when sending information over the Internet	1. Encryption is required when sending information over the Internet
2. E-mail outside of the organization	2. No special handling required	2. No special handling required, but reasonable precautions should be taken	2. Use of e-mail strongly discouraged. Consider using encryption. Broadcast to distribution lists is prohibited. Forwarding only allowed by data owner	2. **Encryption is required.** Broadcast to distribution lists is prohibited**.** . Forwarding only allowed by data owner

Section:	Information Security	Effective:	August 2006
Standard:	Protection by Data Classification	Revised:	
Policy Ref:	5.8.21 Data Classification	Responsibility:	Chief Information Security Officer

	Public	Internal	Confidential	Confidential/High Risk
Display/Print Media (Paper, Film, Fiche, Copiers, Scanners, Video, Cameras,etc.)		*Reasonable precautions to prevent inadvertent disclosure*	*Active measures to prevent unauthorized parties from viewing information*	*Active measures and close control to limit information to as few persons as possible*
1. Printed or digital materials	1. No special precautions required	1. Remove and store out of sight of non-employees including all copies.	1. Remove and store information in a secure location including all copies.	1. Remove and store information in a secure location including all copies.
2. Visual (monitors, screens, LCDs, etc,)	2. No special precautions required	2. Positioned, shielded or presented to prevent viewing by non-employees.	2. Positioned or shielded to prevent unauthorized viewing and use password screen saver, etc.	2. Positioned or shielded to prevent unauthorized viewing and use password screen saver, etc.
Storage				
1. Printed materials	1. No special precautions required	1. Reasonable precautions to prevent access by non-employees	1. Storage in a secure manner, e.g., secure area, lockable enclosure. Must be locked when unattended	1. Storage in a lockable enclosure. Must be locked when not in use
2. Electronic documents	2. Storage on all drives allowed but access controls must be enforced	2. Storage on all drives allowed but access controls must be enforced	2. Store on secure drives or secure shared drives only. Data should be stored on an internally accessible server, and cannot be stored on a server directly accessible from the Internet, such as a public web server	2. Storage on secure drives only. **Password protection of document preferred. Cannot be stored on an Internet web server; data must be stored on a server that is only accessible internally**
3. E-mail	3. No special precautions required	3. Reasonable precautions to prevent access by non-staff & employees	3. Store in a secure manner, e.g. password access or reduce to printed format, delete electronic form, and store in accordance with storage of print materials	3. Store in a secure manner, e.g. password access or reduce to printed format, delete electronic form, and store in accordance with storage of print materials
4. Portable devices	4. No special precautions required	4. Use lockable containers or devices. Where possible use UTHSCSA managed stored encryption solutions	4. Use lockable containers or devices. Where possible use UTHSCSA managed stored encryption solutions	4. Use lockable containers or devices. Where possible use UTHSCSA managed stored encryption solutions

	Public	Internal	Confidential	Confidential/High Risk
5. Storage by business associates (Non-UTHSCSA)	5. No special precautions required	5. Business agreements and non-disclosure agreements required. Secured with lockable enclosures and access controls for only those who have been authorized by UTHSCSA. Annual offsite inspection recommended	5. Business agreements and non-disclosure agreements required. Secured with lockable enclosures and access controls for only those who have been authorized by UTHSCSA. Annual offsite inspection recommended	5. Business agreements and non-disclosure agreements required. Secured with lockable enclosures and access controls for only those who have been authorized by UTHSCSA. Annual offsite inspection recommended
Destruction *(HOP 5.8.22)*				
1. Destruction	1. No special precautions required	1. No special precautions required	1. Destroy in a manner that protects confidentiality	1. Destroy in a manner that protects confidentiality
2. Location of waste paper bins	2. No special precautions required	2. No special precautions required	2. Secure area not accessible to unauthorized persons. Information must be shredded prior to disposal	2. Secure area not accessible to unauthorized persons. Information must be shredded prior to disposal
3. Paper recycling	3. Permitted	3. Permitted, but shredding recommended	3. Prohibited, unless shredded	3. Prohibited unless shredded
4. Electronic storage media	4. No special precautions required. See HOP 5.8.22	4. No special precautions required. See HOP 5.8.22	4. Methods of destruction must be approved by the Information Security Office. See HOP 5.8.22	4. Methods of destruction must be approved by the Information Security Office. See HOP 5.8.22
Physical Security *(HOP 5.8.27)*				
1. Workstations	1. Password screen-saver to be used when briefly unattended. Sign-off work stations or terminals when not in use or leaving work	1. Password screen-saver to be used when briefly unattended. Sign-off work stations or terminals when not in use or leaving work	1. Password screen-saver to be used when briefly unattended. Sign-off work stations or terminals when not in use or leaving work	1. Password screen-saver to be used when briefly unattended. Sign-off work stations or terminals when not in use or leaving work
2. Servers	2. Must be located in secured areas with limited access based on job functions	2. Must be located in secured areas with limited access based on job functions	2. Must be located in secured areas with limited access based on job functions	2. Must be located in secured areas with limited access based on job functions

	Public	Internal	Confidential	Confidential/High Risk
3. Printing	3. No special precautions required	3. Take reasonable precautions in collecting printed material quickly	3. Printing of documents minimized and only when necessary. Unattended printing is permitted only if physical access is used to prevent unauthorized persons from viewing the material being printed	3. Printing of documents when necessary only**. Printers must not be left unattended.** The person attending the printer must be authorized to examine the information being printed
4. Office access	4. No special precautions required	4. No special precautions required	4. Access to areas containing sensitive information must be physically restricted. Sensitive information should be locked when left in an unattended room	4. Access to areas containing sensitive information must be physically restricted. Confidential High Risk information must be locked when left in an unattended room
5. Portable devices: laptops, PDAs, Treos, thumb drives, etc.	5. Computers must not be left unattended at any time without being secured. Places easily accessible by others (hotel, auto, classroom, etc) are not considered secure, thus, lockable solutions are required	5. Computers must not be left unattended at any time without being secured. Places easily accessible by others (hotel, auto, classroom, etc) are not considered secure, thus, lockable solutions are required	5. Computers must not be left unattended at any time without being secured with lockable cables, cabinets, drawers, etc.	5. Computers must not be left unattended at any time without being secured with lockable cables, cabinets, drawers, etc.
Access Control All access control is determined by the data owner *(HOP 5.8.4)*				
1. General	1. Available to the general public. However, content changes must have access controls which allow only those who are authorized for this job function	1. Generally available to all staff on a need-to-know basis. Access rights should have checks and balances with no single point of failure	1. Must have a business need to know the information. Must have approval of the data owner. Should routinely review access to the information. Access rights should have checks and balances with no single point of failure	1. Must have a business need to know the information. Must have approval of the data owner. Must routinely review access to the information. Access rights must have checks and balances with no single point of failure
2. Internal connection	2. Available to the general public. However, content changes must have access controls which allow only those who are authorized for this job	2. Password access control or controlled shares based on general guidance	2. Password access control or controlled shares based on general guidance	2. Password access control or controlled shares based on general guidance. **UTHSCSA managed storage encryption may also be considered**

	Public	Internal	Confidential	Confidential/High Risk
3. UTHSCSA external connection	3. Available to the general public. However, content changes must have access controls which allow only those who are authorized for this job function	3. Prefer encryption via web browser or VPN access with user authentication and managed roles	3. Encryption via web browser or VPN access with user authentication and managed roles	3. Encryption via web browser or VPN access with user authentication and managed roles
4. Non-UTHSCSA	4. Available to the general public. However, content changes must have access controls which allow only those who are authorized for this job function	4. Must be approved by the data owner prior to access. Encryption via web browser or VPN access with user authentication and managed roles	4. Business agreements and non-disclosure agreements required prior to access. Encryption via web browser or VPN access with user authentication and managed roles	4. Business agreements and non-disclosure agreements required prior to access. Encryption via web browser or VPN access with user authentication and managed roles

	Public	Internal	Confidential	Confidential/High Risk
Backup and Recovery *(HOP 5.8.23)*	• Should be backed up monthly and incrementally based on content change • Monthly and incremental backups should remain separate processes and labeled accordingly • Never overwrite the most recent backups • Should be able to restore in a timely manner from a partial disaster or a full disaster as required for business operations • Backups should be kept in a secured location • Backups should be tested regularly to ensure reliability • Must comply with records retention requirements	• Should be backed up monthly and incrementally based on information recovery requirements by data owners and business operational needs • Monthly and incremental backups should remain separate processes and labeled accordingly with tracking controls • Never overwrite the most recent backups • Should be able to restore in a timely manner from a partial disaster or a full disaster as required for business operations • Backups should be kept in a secured location • Backups should be tested regularly to ensure reliability • Must comply with records retention requirements	• Should be backed up monthly and incrementally based on information recovery requirements by data owners and business operational needs • Monthly and incremental backups should remain separate processes and labeled accordingly with strict tracking controls • Never overwrite the most recent backups • Should be able to restore in a timely manner from a partial disaster or a full disaster as required for business operations • Backups should be kept in a secured location • Backups should be tested regularly to ensure reliability • Access to backups should be controlled and authorized by data owners • Courier services must be trusted sources and authorized by data owners • Must comply with records retention requirements	• Must be backed up monthly and incrementally based on information recovery requirements by data owners and business operational needs • Monthly and incremental backups must remain separate processes and labeled accordingly with strict tracking controls • Never overwrite the most recent backups • **Must** be able to restore in a timely manner from a partial disaster or a full disaster as required for business operations • Backups **must** be kept in a secured location • Backups **must** be tested regularly to ensure reliability • Access to backups **must** be controlled and authorized by data owners • Courier services must be trusted sources and authorized by data owners • Must comply with records retention requirements

	Public	Internal	Confidential	Confidential/High Risk
Lost, Disclosed, or Stolen				
1. Data	1. No special requirements, but should be restored from a valid backup as soon as possible	1. Should be reported to departmental TSRs	1. Immediately notify the Information Security Office, 210-567-5900	1. Immediately notify the Information Security Office, 210-567-5900
2. Physical	2. Notify University Police, 210-567-2800	2. Notify University Police, 210-567-2800, and departmental TSRs	2. Immediately notify University Police, 210-567-2800, and the Information Security Office, 201-567-5900	2. Immediately notify University Police, 210-567-2800, and the Information Security Office, 201-567-5900