

Attachment I

Data Security, Management, Use, And Disposition Requirements Based On Data Classification

	Unclassified	Operational Use Only	Confidential
Data Access Approval (read, write, add, update, delete access)	No special requirements	Data Custodian approval needed	Data Custodian approval needed
Distribution of data regardless of method or media	No special requirements or limits	Data Custodian to define requirements	Minimum distribution on a “need to know” basis Redact unnecessary Confidential information
Transport of data between sites	No special requirements	No special requirements	Use reliable transport or courier Package securely (e.g., use locked container, tamper proof container, Splitting information into more than one package) Signoffs For The Physical Transport Of Media Exists at both ends of transport
Data transmitted via FAX	No special requirements	Data Custodian to define requirements	Redact unnecessary Confidential information Send FAX from secure area by authorized personnel only Send a test fax to the recipient prior to sending confidential information and verified recipient received test fax Attend at receiving FAX
Data transmitted via wide area network (WAN) or local area network (LAN)	No special requirements	No special requirements, encryption optional	Redact unnecessary Confidential information Transmitted in encrypted form or other appropriate and equally secure method Confirmation of receipt required
Data transmitted via Mail (Campus or U.S. Postal)	No special requirements	No special requirements	Redact unnecessary Confidential information Label envelope and document as “Confidential – To Be Opened by Recipient Only”

Attachment I

Data Security, Management, Use, And Disposition Requirements Based On Data Classification

	Unclassified	Operational Use Only	Confidential
Data transmitted via voice mail or on answering machine	No special requirements	No special requirements	Place call from secure area not from open office area or public space Confirmation that message left on voice mail system or answering machine is secured (e.g., password protected, not a shared “mailbox”) and inaccessible by other than the intended recipient. Confirmation to sender that data received. Remove message after receipt
Data transmitted via email	No special requirements	Data Custodian to define requirements	Redact unnecessary Confidential information Transmitted in encrypted form or other appropriate and equally secure method Confirmation of receipt required
Data transmitted by wireless or cellular phone	No special requirements	Data Custodian to define requirements	Do not transmit
Use of data	No special requirements	No special requirements	Data not to be left visible on screen or desk Secure data when not in use Clear work area (i.e., desk, in and out trays, etc.) at the end of each working day, and file documents appropriately Redact unnecessary Confidential information when sharing data
Storage on fixed media (e.g., server, hard drive, etc.)	No special requirements	Unencrypted	Unencrypted if access to fixed media is controlled Encrypted if access to fixed media is NOT controlled

Attachment I Data Security, Management, Use, And Disposition Requirements Based On Data Classification

	Unclassified	Operational Use Only	Confidential
Storage on removable media (e.g., diskette, CD-ROM, magnetic tapes, USB, etc.)	No special requirements	Data Custodian to define requirements	Unencrypted if access to removable media is controlled Encrypted if access to removable media is NOT controlled All media removed from the University shall be logged and transported securely
Storage on temporary device/spool	No special requirements	Data Custodian to define requirements	Secure data, limit access to authorized personnel only
Storage on hardcopy	No special requirement	Data Custodian to define requirements	Stored in secure cabinet with access by authorized personnel only
Use of carbon paper in hardcopy creation	Trash/Recycle	Trash/Recycle	Cross-shred, chemically destroy or incinerate in an environmentally safe method
Printing hardcopy of data	No special requirements	Data Custodian to define requirements	Output to be routed to a pre-defined, monitored or secure printer Output not left on printer
One time use printer ribbons	Trash/Recycle	Trash/Recycle	Destroy or incinerate in an environmentally safe method
External labeling of exchangeable media (print, disks, cds, tapes, cassettes etc.)	No special requirements	Data Custodian to define requirements	Label - note owner and as "Confidential"
Internal labeling of information at the application or screen/page/panel level	No special requirements	Data Custodian to define requirements	Notification of "Confidential Data" to appear at top of screen/page/panel

Attachment I

Data Security, Management, Use, And Disposition Requirements Based On Data Classification

	Unclassified	Operational Use Only	Confidential
Disposal of removable electronic media (e.g., diskettes, CDs, DVDs, optical disks, magnetic tapes, etc.)	<p>Migrate files contained on hardware or electronic storage devices that are not past their retention period to current systems or another suitable storage format</p> <p>No special disposal requirements</p>	<p>Data Custodian to define requirements</p>	<p>Sanitize</p> <p>Shred CDs and DVD's</p> <p>If the custodial department is not sure if the medium contains such information, the medium shall be sanitized to ensure no sensitive data may be disclosed</p> <p>Log time, date, method and person that disposed of media</p>
Disposal of hard drive	<p>Migrate files contained on hardware or electronic storage devices that are not past their retention period to current systems or another suitable storage format.</p> <p>“Wipe”/Sanitize functioning hard-drives.</p> <p>If cpu to be destroyed, physically remove and destroy ALL hard drives.</p> <p>Log time, date, method and person that disposed of media</p>	<p>Migrate files contained on hardware or electronic storage devices that are not past their retention period to current systems or another suitable storage format.</p> <p>“Wipe”/Sanitize functioning hard-drives.</p> <p>If to cpu to be destroyed, physically remove and destroy ALL hard drives.</p> <p>Log time, date, method and person that disposed of media</p>	<p>Migrate files contained on hardware or electronic storage devices that are not past their retention period to current systems or another suitable storage format.</p> <p>“Wipe”/Sanitize functioning hard-drives.</p> <p>If cpu to be destroyed, physically remove and destroy ALL hard drives.</p> <p>Log time, date, method and person that disposed of media</p>

Attachment I
Data Security, Management, Use, And Disposition Requirements Based On
Data Classification

	Unclassified	Operational Use Only	Confidential
Disposal of hardcopy	Trash/Recycle	Trash/Recycle	Cross-shred, chemically destroy or incinerate paper, microfiche and microfilm in an environmentally safe method. Log time, date, method and person that disposed of media
Review of information for reclassification (classifications of information assets may change over time)	Data Custodian to determine specific review date (not to exceed one year)	Data Custodian to review annually	Data Custodian to review annually
Auditing Access Activity	No special requirements	Data Custodian to define requirements	Log all access attempts (successful and unsuccessful) noting access type (i.e., read, add, update, delete) Log reviewed by Data Custodian
Access Activity Audit Log Retention	No special requirements	Data Custodian to define requirements (not to exceed 6months)	Retain audit log for 6 months or as needed for ongoing investigation

Return to [University Data and Computing Standards](#)