TRS Confidential Information Procedures & Standards

INTRODUCTION

To supplement the TRS *Confidentiality Policy*, the following procedures and standards were created to provide general guidelines for TRS employees and non-TRS workers to follow and to help management enforce the policy. All TRS employees and non-TRS workers with access to confidential information are responsible for identifying, classifying, protecting, and appropriately disposing of this information in accordance with the following procedures and standards. Unauthorized disclosure or access of confidential information is subject to corrective action, sanction, or penalty as outlined in the *Confidentiality Policy* and *TRS Personal Trading Policy*.

INFORMATION CATEGORIES & RECORD COPIES

Information designated by TRS as “confidential” includes the following information categories: **confidential by law**, **HIPAA**, **sensitive**, and **vital** or **critical** information. These procedures and standards are specific to TRS information classified as **high risk** according to the *Information Security Manual (ISM),* Section 6.3 (Classifying TRS Information). High risk information requires a higher level of protection than information classified as medium or low risk. For a quick reference table that provides general standards and guidance for protecting TRS confidential information as well as guidance on medium to low risk information, see **Appendix A**, page 6 (*TRS’ Information Protection Standards*).

The record copy of confidential information must be retained and disposed of in accordance with TRS’ *Records Management Program Policy,* procedures, and retention schedules. In this document, including the table below, directions to immediately destroy or otherwise dispose of confidential information or the media on which it resides applies only to convenience copies of such information or media.

CONFIDENTIAL INFORMATION

For TRS business purposes, high risk information is designated “confidential” but may not be specifically confidential by law, rule, or regulation. Legally, information that is “confidential by law” is information that TRS is prohibited from releasing and its disclosure is subject to criminal penalties. Other law may *permit* TRS to withhold certain information at TRS’ discretion but does not make disclosure subject to criminal penalties.

In accordance with TRS policies and procedures and, as appropriate, in consultation with the Executive Council or a director, information owners may exercise discretion in releasing information pursuant to a permissive law. But in implementing the *Confidentiality Policy* and these procedures, TRS employees and non-TRS workers must handle information subject to permissive release as if it were confidential. In addition, this policy and procedures treat the other information categories covered by them as “confidential” to facilitate compliance with the policy and implementation of the procedures by information owners, employees, and non-TRS workers.

GENERAL PROCEDURES FOR HANDLING TRS CONFIDENTIAL INFORMATION	
Access (includes access to read, update, delete, view, change, add, remove,	Electronic and physical access to confidential information is restricted and only authorized for employees and non-TRS workers with the minimum necessary access for them to perform their assigned duties or to conduct TRS business. Electronic access includes network drives, folders, applications, and web portals. *Do not share security badges or disclose user IDs or passwords.*

GENERAL PROCEDURES FOR HANDLING TRS CONFIDENTIAL INFORMATION	
copy, move, or replace files—all of these or any combination of these)	*Immediately remove access to web portals when employees or non-TRS workers terminate.*
Classify	Information assets are classified as high risk, medium risk, or low risk as defined in the *ISM,* Section 6.3 (Classifying TRS Information). Information owners are responsible for identifying and classifying information for their divisions and departments. Employees and non-TRS workers, with guidance from their designated information owners, are responsible for identifying and classifying information. See **Appendix B**, page 10, for examples of *TRS High Risk Classification Records*. On a biennial basis, information owners recertify information classified as high risk by reviewing and updating their departmental/divisional Data Protection Policy & Procedures document, including the corresponding data protection worksheet.
Store	***Electronic copy*** – Store confidential information in restricted access folders within your department's network folder (S:\ drive), restricted access team folder (S:\Teams), password-protected folder, or restricted collaboration SharePoint library. Do not store these records, convenience copies or working files on the local C:\ drive, G:\ drive or S:\AllTRS. Follow the department's established file folder structure to maintain the official business documents and protect confidential information. Confidential information should be logically and physically separated from **public** information to ensure its protection is at the high risk classification level. When practical, electronic confidential information is password-protected by individual file, file folder, or is labeled "**CONFIDENTIAL**" within the electronic document for quick identification and monitoring. Watermarks, footers, headers or other formatting may be used. Removable media require encryption and secure storage. Employees and non-TRS workers must use encryption techniques before storing confidential information on removable media such as a USB flash drive, CD, or DVD. Contact the Helpdesk for encryption assistance. Refer to the *ISM,* Section 8.5 (Information Encryption) for further information. The information owner or custodian of the information resource will ensure confidential information stored on mainframe applications and other systems or software has restricted access controls in place such as authentication level security which requires password-protection. Refer to the *ISM*, Section 5.4 (Password Management) for further information. Criminal history record information should never be stored electronically (including in restricted folders).

GENERAL PROCEDURES FOR HANDLING TRS CONFIDENTIAL INFORMATION	
	Hardcopy – Hardcopy confidential information is stored out of sight of unauthorized persons and organized and identified by file drawer or file folder in a lockable cabinet, desk drawer, or other secure area. When practical, confidential information is labeled "**CONFIDENTIAL**" on the hardcopy document or different color paper (i.e., pink copy paper) is used for quick identification and monitoring.
Protect (includes printing, copying, and releasing)	Confidential information must be protected at all times and must not be left unattended on desks, computers, copiers, printers, scanners, or fax machines. Printing and copying is limited and only as needed for business purposes. Copies are immediately destroyed (shredded) after the confidential information has served its purpose or in accordance with the *Records Management Program Policy*. Prior to releasing confidential information for open records requests or other requests, the information owner, chief officer or director authorizes and documents the release electronically or in writing. Criminal history record information may be printed by authorized persons on a case-by-case basis. A hardcopy is provided to the Chief Human Resources Officer (CHRO) if a criminal history is revealed. The CHRO consults with the Deputy Director and Legal & Compliance. Upon completion of review, the hardcopy criminal history record information is properly destroyed (shredded).
Communicate (includes verbal, visual, and Social Media)	Confidential information is communicated only on a need-to-know basis to perform assigned duties or to conduct TRS business. Refer to **Appendix A**, page 6, for specific standards on communicating confidential information. As outlined by the *Social Media Policy*, posting confidential information to social media websites is not permitted.
Transmit (includes faxing, electronic, and wireless or mobile devices)	Electronic confidential information requires encryption prior to external transmission or is transmitted using a secured VPN, SFTP, or TLS. Review email distribution lists or email addresses to ensure the information reaches the appropriate persons/entities. Contact the Helpdesk for assistance with encrypting information prior to electronic transmission. Do not fax confidential information to any party unless this method has been approved by your manager. Employees and non-TRS workers must use encryption techniques before communicating confidential information using cell phones, laptops, or other mobile devices. For further information, refer to the *ISM*, Section 3.1 (Acceptable Use of Information Resources) and *B.2. Standards, Disclosure and Use of TRS Information* which outlines certain methods of communication that are prohibited or are only allowed if using approved encryption techniques.

GENERAL PROCEDURES FOR HANDLING TRS CONFIDENTIAL INFORMATION	
	Criminal record history information must never be transmitted internally or externally.
Mail	Review mailing addresses to ensure the confidential information is sent to the appropriate person/location. When sending mail via interoffice or inter-agency mail, use two envelopes. For the inside envelope, place the hardcopy information inside it securely sealed, mark it "**CONFIDENTIAL**." For the outside envelope, mark it as you normally would with the recipient's name, giving no indication of the confidentiality of the information it contains. When sending mail using an external mail service, use a bonded courier or mail the information using a securely sealed inside container/envelope marked "**CONFIDENTIAL**" and an outside unmarked container/envelope. Return receipt or certified receipt can also be used to track delivery.
Dispose	To dispose of confidential information, locked shred bins are located in each copy room. Designated employees on some floors have key access to these shred bins for high volume disposal. The bin is emptied once a week by Staff Services. Shredders are also available in some copy rooms and departments to destroy documents immediately or in accordance with the *Records Management Program Policy*. Black confidential shred bins should also be emptied prior to leaving work each day. Electronic (soft) information should be disposed of in accordance with the records retention schedule and hardware, such as removable media, needing immediate destruction must be placed in the appropriate electronic media disposal bin located in the Information Technology division. Prior to disposing removable media, fax machines, copiers, computers, or other electronic devices, ensure that the internal disks are properly cleansed, destroyed, or shredded.
Monitor Compliance	Information owners and the Information Security Officer are responsible for monitoring compliance with classifying and protecting confidential information. Monitoring compliance includes the following: • Periodic review of access to information resources and physically restricted areas to ensure access is only granted to perform assigned duties or to conduct TRS business. • Periodic review of shared network drives and shared folders for inappropriate placement of confidential information.

GENERAL PROCEDURES FOR HANDLING TRS CONFIDENTIAL INFORMATION	
	• Conducting walk-throughs of areas most likely to have this type of information visually and physically available to unauthorized TRS employees, non-TRS workers, and members or retirees. In addition, the Information Security Officer performs an annual security risk assessment to identify and provide recommendations on vulnerabilities, risks, and other security threats related to confidential information on TRS information resources.
Report Noncompliance & Security Incidents	Immediately report noncompliance with these procedures to your designated information owner or manager and the Information Security Officer. Non-TRS workers must report noncompliance with these procedures to their contract sponsor. • If a hard copy document with PII and/or PHI is lost or stolen, notify your manager so that appropriate action can be taken immediately. • When a laptop or other mobile device is lost or stolen, immediately notify the appropriate IT security personnel so that the laptop/device can be remotely wiped by IT staff timely. • If an unauthorized disclosure or access of HIPAA or confidential information is suspected, immediately contact the following: ▪ Privacy Officer in Legal & Compliance (HIPAA information) ▪ Information Security Officer (Confidential information—non-HIPAA) • If unauthorized disclosure or access of criminal history record information is suspected, immediately contact the following: ▪ Chief Human Resources Officer ▪ Assistant Director of Human Resources ▪ Information Security Officer (Confidential information—non-HIPAA) Refer to the *ISM*, Section 4.0 (Reporting Information Resources Security Incidents) for further guidance.
Train & Educate	Managers ensure training is provided to new employees within 30 days of employment and biennially thereafter for current employees. Departmental/divisional specialized HIPAA training is provided annually and documentation of completion is maintained by Human Resources. Contract sponsors will ensure non-TRS workers are provided individual training on confidentiality and HIPAA according to the *Non-TRS-Worker Intake and Exit Procedures.*

APPENDIX A – TRS' Information Protection Standards

	HIGH RISK				MEDIUM-LOW RISK
	Confidential by Law	**HIPAA**	**Sensitive**	**Vital/Critical**	**Public**
Information Categories & Definitions	Information maintained by or for TRS that is protected from disclosure by state or federal law or regulation or by TRS policy and procedures.	Protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996, which may include personally identifiable information (PII) and individually identifiable health information (IIHI).	Information maintained by TRS that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness.	Information that is necessary to resume or continue TRS' business; to recreate its legal and financial status or preserve the rights of TRS, its employees, and its participants. Information determined to be essential to TRS' mission and functions, the loss of which would have a significant negative impact.	Not deemed "confidential" under TRS' *Confidentiality Policy* or Confidential Information Procedures & Standards.
Information Examples *(For a detailed list of high risk classification records, see **Appendix B**, page 10)*	• Member and retiree records, information, or correspondence (including annuities, benefits, demographics, payroll) • Investment due diligence materials and information on external, private investments (pre and post) • Material non-public information • Social Security numbers • Account information (including PINS) of bank,	• Medical information • Benefits appeals cases and related member medical information	• Broker information • Personally identifiable information (PII) including home and email addresses • Member satisfaction surveys	• Contracts and related information • Legal matters and negotiations (including attorney-client communications) • Litigation information (pending or anticipated)	• Information made available on TRS' public Internet site • Records released in response to Open Records requests

APPENDIX A – TRS' Information Protection Standards

	HIGH RISK				MEDIUM-LOW RISK
	Confidential by Law	HIPAA	Sensitive	Vital/Critical	Public
	credit, and charge or debit cards • Criminal history record information				
Access Control	Electronic and physical access is restricted to authorized employees and non-TRS workers; only authorized with the minimum necessary access to perform assigned duties or to conduct TRS business. Electronic access includes network drives, folders, applications and web portals. *Do not share security badges or disclose user IDs or passwords. Immediately remove access to web portals when employees or non-TRS workers terminate.*				Open access
Communication (verbal, visual, or social media): • Conversations/ meetings • Monitors/Screens • Cell phones/phones • Presentation slides • Voicemail • Online posts	To prevent unauthorized disclosure: a) Maintain low voices. b) Avoid conversations in public areas such as elevators, hallways, or at social gatherings. c) Speakerphone use only in limited, restricted, or secured area. d) Limit information in presentations and voicemails. e) Anonymize confidential identifying information by substituting reference numbers or other words. f) Excuse unauthorized persons from discussions on confidential information. g) Prior to using a cell phone, approved encryption techniques must be used. h) Position monitors and printers so that unauthorized persons cannot see or obtain the information. i) Use password-protected screensavers, log out or shut down when leaving your computer unattended at any time. j) Do not post confidential information to social media websites.				Verbal, visual, or online posting protection is not required.
Transmission* (internal/external mail, email, or fax) *Employees and non-TRS workers must <u>use</u>	***External transmission:*** Use secured VPN, SFTP, or TLS for electronic submissions sent over unsecured or public networks. Contact the Helpdesk for encryption assistance. ***Fax:*** Use dedicated fax transmission directly to recipient or convert fax to PDF and send encrypted email. Do not fax confidential information to any party unless this method has been approved by your manager. ***Email:*** • Emails, text messages, and instant messages are sent encrypted or password-protected.				Transmission protection or encryption is not required.

APPENDIX A – TRS' Information Protection Standards

	HIGH RISK				MEDIUM-LOW RISK
	Confidential by Law	HIPAA	Sensitive	Vital/Critical	Public
approved encryption techniques before communicating confidential information using laptops, mobile devices, or removable media.	• Review email distribution lists or email addresses to ensure information reaches appropriate person/entity. • Anonymize confidential identifying information by substituting reference numbers or other words. • In Outlook, set the message settings sensitivity to "Confidential." ***Mail:*** • Review mailing addresses to ensure information is sent to the appropriate person/location. • Use two envelopes/containers; inside envelope/container is securely sealed, marked "**CONFIDENTIAL**," and the outside envelope/container is unmarked with normal address information giving no indication of its confidentiality. • Use non-window envelopes or security-tinted envelopes. • Track mail using return receipt or certified receipt. • Use password-protected or encrypted removable media such as a USB drive, CD, or DVD; approved encryption techniques are required. ***Physical Delivery:*** Hand-deliver to addressee or use bonded courier mail service. ***Criminal record history information:*** Must never be transmitted internally or externally or accessed when working remotely.				
Printing, Copying, and Releasing: • Printed/hardcopy materials • Open Records/ Other Requests	a) Shield to prevent unauthorized disclosure. b) Do not leave unattended on desks, computers, copiers, printers, scanners, or fax machines. c) Printing and copying is limited and only when needed for business purposes. d) Copies must be protected in the same manner as the original. e) Copies are immediately destroyed (shredded) after the information has served its purpose or in accordance with the *Records Management Program Policy.* f) Prior to releasing for open records requests or other requests, the information owner, chief officer, or director authorizes and documents the release in writing or electronically.				No restrictions to copy, print, or release public information.
Storage: • Hardcopy/Electronic documents • Email	a) Store out of sight of unauthorized persons, under lock and key, or in a secured area. b) Store in restricted access folders such as the S:\ drive, S:\Teams, password-protected folder, or restricted collaboration SharePoint library. Do not store these records, convenience copies or working files on the local C:\ drive, G:\ drive or S:\AllTRS.				No restrictions on location or placement of public information.

APPENDIX A – TRS' Information Protection Standards

	HIGH RISK				MEDIUM-LOW RISK
	Confidential by Law	**HIPAA**	**Sensitive**	**Vital/Critical**	**Public**
• Removable media	c) Storing on removable media requires encryption protection and secured storage. d) When practical, hardcopy and electronic documents are labeled "**CONFIDENTIAL**" for quick identification and monitoring. Watermarks, footers, headers, other formatting, or different color paper may be used (i.e., pink copy paper). e) Email is protected in the same manner as printed materials; use password-protected screensaver when you are away from your computer. f) When storing offsite, the offsite facility must be bonded. g) Criminal history record information should never be stored electronically (including in restricted folders).				
Disposal: • Shred bin • Removable media (drives/tapes/USB/ CD/ DVD) • Hardware • E-Records Purge	Shred bin is in a secure area or securely locked. a) Shred copies immediately after business use or in accordance with the *Records Management Program Policy.* b) Place confidential documents in locked shred bin. Black confidential shred bins should also be emptied prior to leaving work each day. c) Electronic (soft) information should be disposed of in accordance with the records retention schedule and hardware, such as removable media, needing immediate destruction must be placed in the appropriate electronic media disposal bin located in the Information Technology division. d) Ensure internal disks/media are properly cleansed, destroyed, or shredded prior to disposing removable media, fax machines, copiers, computers, or other electronic devices.				Place information in unlocked recycle bin or trash can.

APPENDIX B – TRS HIGH RISK CLASSIFICATION RECORDS

TRS' **high risk** classification contains the following records that may typically include some confidential information. For a more detailed listing of confidential information, please refer to the Data Protection Policy & Procedures for each subject area.

SUBJECT AREA	RECORDS
Benefits **Health Insurance** **Member Information** **Records Management**	▪ Association mailings ▪ Benefits appeals cases and related member medical information ▪ Disease state outlier reports ▪ Elected insurance coverage and financial options (including insurance policy numbers) ▪ Enrollment information (health benefit programs) ▪ Medical information--protected health information (PHI) under HIPAA and individually identifiable health information (IIHI) ▪ Member, retiree, and beneficiary records, information, or correspondence (including alternate payees, annuities, benefits, demographics, or payroll) ▪ Member satisfaction surveys ▪ Records due for destruction per TRS Records Retention Schedule ▪ Retiree Drug Subsidy (RDS) and Early Retiree Reinsurance Program ▪ Vendor medical and RX claims ▪ Vendor medical claims audit reports
Board of Trustees	▪ Board of Trustees (confidential board meeting materials and board elections information)
Contracts **Financial**	▪ Account information (including PINS) of bank, credit, and charge or debit cards ▪ Contracts and related information ▪ Vendor pricing
Human Resources	▪ Driver's license numbers ▪ Employee personnel files (360 reviews, appraisals) ▪ Personal, non-public information of TRS employees, former employees, job applicants, and Board of Trustees members ▪ Personally identifiable information (PII) including birthdates, birth certificate, home and email addresses, or telephone numbers ▪ Social Security Numbers ▪ Medical and other information subject to the Americans with Disabilities Act (ADA) ▪ Medical and other information related to HIV/AIDS ▪ Workers' Compensation information ▪ Medical and other information subject to the Family and Medical Leave Act (FMLA) ▪ Equal Employment Opportunity (EEO) information ▪ Sexual Harassment Reports ▪ Criminal history record information
Investments	▪ Asset allocation changes affecting market prices for public securities ▪ Broker information ▪ Investment agreements and transaction details (subject to confidentiality agreements) ▪ Investment due diligence materials and information on external, private investments (pre and post) ▪ Investment fund information and records (credit reports, performance history, or background information) ▪ Investment reporting materials, transparency reports, Internal Investment Committee (IIC) meetings and minutes ▪ Material non-public information ▪ Proprietary business information/research, models, and reports ▪ Trade secrets or other confidential commercial or financial information

	▪ Trading data and due diligence information (real-time, pre and post) ▪ Trust positions by Asset Class
Audit **Fraud/Ethics** **IT/Risk Management**	▪ Audit working papers ▪ Fraud and ethics hotline reports and investigations ▪ Risk or vulnerability assessments (information systems)
Legal	▪ Legal matters and negotiations (including attorney-client communications) ▪ Litigation information (pending or anticipated)
Payroll	▪ Social Security Numbers ▪ Bank routing numbers ▪ Withholding amounts ▪ Insurance selection ▪ QDRO ▪ Garnishments
Non-Public Information	▪ Information not made public about TRS or another entity.