# Managing Mobile Media And The Secure Transport Of Ingress And Egress Data In Closed Environments

## Suggestions for Operational Procedures To Securely Transfer Files Using Tresys XD Air

XD Air™

TRESYS TECHNOLOGY

Owl Cyber Defense, LLC
8840 Stanford Boulevard
Columbia, MD 21045

# 1 INTRODUCTION

This guide presents a starting point for the creation of a series of procedures for the management and tracking of data and data media destined for and originating from Digital Assets. Throughout the data transfer process, it remains imperative to handle externally sourced data media in a manner isolating these devices from direct interaction with Digital Assets.

This document has been developed as a guide template for licensees in conjunction with Nuclear Energy Institute document "Cyber Security Plan for Nuclear Power Reactors" (NEI 08-09) to comply with the requirements of 10 CFR 73.54. The goal is act as a starting point "to facilitate the implementation of the media protection policy and associated media protection controls which include the methodology that defines the purpose, scope, roles, responsibilities, and management commitment in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal necessary to provide a high assurance that the risk of unauthorized disclosure [or introduction] of information that could be used in a cyber-attack to adversely impact the safety, security, and emergency preparedness functions of the nuclear facility is prevented" (quote from NEI 08-09 Appendix E.1, Media Protection).

The adoption of new technology provides many benefits including better data analysis tools and reporting, higher efficiencies, and quicker turn-around in troubleshooting and repair. With these benefits, it is becoming increasingly important be able to pass data to and from systems that reside in locations isolated from general access networks.

This guide provides a *basic* procedural structure for the management of data media intended for Digital Assets both for inbound "ingress" data (for example, introducing software updates) or for outbound "egress" data (for example, extracting troubleshooting log files). This template emphasizes fully documented tracking of data media (for example, CD/DVDs and USB drives) and the separation of data media sourced from external entities from the data media used with restricted Digital Assets.

# 2 GLOSSARY/DEFINITIONS

## 2.1 Digital Asset

Any digital computer, communication system or network, control system or any other system used in the operation of the location or facility. Legacy "analog" systems should also be included if the system has a digital interface (ex. used for updating features or log exporting)

## 2.2 Data Ingress

The process by which new data may be brought in to a given location or facility. For example, digital asset software updates. This includes file types of all kinds (ex. text configuration files, updates, executables, programs, Microsoft Office documents, pdfs, images, etc.)

## 2.3 Data Egress

Data (or, more likely, a copy of the data) to be removed from the location or facility. For example, logging, status or error reports. This includes file types of all kinds (ex. text configuration files, updates, executables, programs, Microsoft Office documents, pdfs, images, etc.).

## 2.4 Media

Media is generally used for the storage (temporary or long-term) or transport of digital data. Media includes but is not limited to:

- Optical media
  - CD-ROM
  - CDR
  - CD±RW
  - DVD-ROM
  - DVD±RW
- USB flash drives
- CompactFlash cards
- SD cards
- External hard drives (via USB, SATA, eSATA, etc.)
- External solid state drives (via USB, SATA, eSATA, etc.)
- Floppy disks
- Other devices with data storage capability (such as mobile phones, MP3 players, etc.) attached via USB, Firewire, etc.

## 2.5 Media source

2.5.1 The entity, individual, company, etc. that is responsible for media and the data contained thereon. For example, the media source for a digital asset software update would be the associated vendor. As another example, the media source could be an internal software development group that creates new operational configuration files.

2.5.2 Local requirements may dictate the expansion of these procedures to accommodate a delineation of media sources.

2.5.2.1 Internal media sources include those individuals within the jurisdiction of the location security authority.

2.5.2.2 External media sources certainly include entities outside the licensee company (ex. vendors), but may also include licensee employees, contractors, representatives, etc. from other licensee locations.

## 2.6 Media Pool

The media pool is a closely controlled set of clean, blank, securely erased, and reformatted media that are made available for use within a secured area. All media within the pool has previously been

checked-in, following the complete check-in procedure (inventory entry, tagging and tracking, cleaning, etc.). Media removed from the pool must follow the complete check-out procedure (inventory tracking, etc.).

## 2.7 Secure Erased Media

The Secure Erase process overwrites all accessible media blocks present on the storage device using a methodology provided by the Government to accomplish complete erasure. The media is then reformatted.

# 3 REQUIREMENTS

The procedures in this guide template must be implemented and modified as necessary for complete compliance with location and facility security policies.

# 4 PROCESSES FOR DATA MEDIA MANAGEMENT

The complete life-cycle management of data media minimizes security exposure for internal Digital Assets. These management processes detail the proper usage and tracking of data media. These processes are built on elemental Procedures given in Section 6.

## 4.1 New Media

This process is for newly acquired unused media for inclusion in the media pool.

4.1.1 Register media in Media Inventory Tracking (see 6.1.1)

4.1.2 Check-In media to Media Pool (see 6.2)

## 4.2 Retire Media

This process is for the handling of unusable media.

4.2.1 Dispose of media (see 6.8)

## 4.3 Data Ingress

This process details the steps for the introduction of external data to a Digital Asset

4.3.1 Register external media in Media Inventory Tracking (see 6.1)

4.3.2 Check-out available internal media from Media Pool (see 6.3)

4.3.3 Data Transfer from external to internal media (see 6.6)

4.3.4 Quarantine external media (see 6.7)

4.3.5 Use internal media for data ingress to Digital Asset

4.3.6 Scan internal media for infection (see 6.5)

4.3.6.1 If media is not clean notify local Security authorities

4.3.7 Check-in internal media (see 6.2)

4.3.8 Dispose of external media (see 6.8)

## 4.4 Data Egress

This process details the steps for the exporting of data from a Digital Asset

4.4.1 Check-out available media from Media Pool (see 6.3)

4.4.2 Extract Egress Data from Data Asset using checked-out media

4.4.3 Scan media for infection (see 6.5)

4.4.3.1 If media is not clean notify Security Department

4.4.4 Determine media destination

4.4.4.1 If media is to be removed from facility follow 6.8

4.4.4.2 If media is to be transferred to external media

4.4.4.2.1 Register external media in Media Inventory Tracking (see 6.1.1)

4.4.4.2.2 Transfer Data from internal to external media (see 6.6)

4.4.4.3 Check-in internal media (see 6.2)

4.4.4.4 Dispose of external media (see 6.8)

## 4.5 Lost Media

This process details the handling of lost media (internal or external)

4.5.1 Notify owner or responsible entity

4.5.2 Update Media Tracking information.

## 4.6 Found Media

This process details the handling of found media (internal or external)

4.6.1 Notify owner or responsible entity

4.6.2 Update Media Tracking information.

4.6.3 Internal media

4.6.3.1 Scan internal media for infection (see 6.5)

4.6.3.1.1 If media is not clean notify Security Department

4.6.3.2 Check-in internal media (see 6.2)

4.6.4 External media

4.6.4.1 Dispose of external media (see 6.8)

# 5 PROCEDURES

The proper handling of data and associated media has been broken down into elemental procedures. The day-to-day operational processes (Section 5) built from these procedures.

## 5.1 Media Inventory Tracking

The tracking the location and life-cycle of all media is central to the management and safe use of mobile media. This is particularly important in any post-event forensic analysis. A centralized easily accessible (possibly web-based) database would be ideal. Updates to the tracking data should be time-stamped.

5.1.1 Media registration

Information identifying the media and its use should be recorded, including but limited to:

5.1.1.1 Ownership

The ownership of the media should specify whether this is intended for the internal media pool or from external sources, whether the media ownership will be transferred (ex. the vendor provides the media to be kept by local personnel left onsite.

5.1.1.2 Media identification (as applicable)

- Type (USB flash, DVD, etc.)
- Brand
- Model
- Serial number

5.1.1.3 Tagging

All media should be tagged to permit tracking, including but not limited to:

- Owner
- Local responsible individual
- Assigned unique tracking number
- “If found…” contact information

5.1.2 Track life-cycle of media intended for media pool and external media

5.1.2.1 Check-in

Tracking should include the name of the responsible person.

5.1.2.2 Check-out

Tracking should include the name of the responsible person, the intended use of the media and identification of digital assets to be used with the media.

5.1.2.3 Scanning

Tracking should indicate the success or failure and the name of the responsible person.

5.1.2.4 Cleaning

Tracking should include the name of the responsible person.

5.1.2.5 Media disposal

Tracking should include the name of the responsible person, the reason for disposal and the final means of disposition.

## 5.2 Check-In

This process returns or adds new media to the media pool.

5.2.1 Check-in is applicable to new and used media

5.2.2 Clean the media.

5.2.2.1 If the media fails this, dispose of media (see 6.8)

5.2.3 Physically return the media to media pool location.

5.2.4 Update media tracking information.

## 5.3 Check-Out

The process temporarily or permanently removes media from the media pool.

5.3.1 Remove the media from the pool.

5.3.2 Update media tracking information.

## 5.4 Cleaning

This process ensures the media is free from unintended data. Generally, the media is completely rewritten with useless data (for example, all zeros) and then reformatted. The Tresys Technology XD Air product provides a complete secure erasure and reformatting of media.

5.4.1 Follow vendor procedures for cleaning the data media.

5.4.1.1 If the media fails this, dispose of media (see 6.8)

5.4.2 Update media tracking information.

## 5.5 Scanning

This process non-destructively analyses media for unintended data including viruses, malicious code, non-policy filetypes, obfuscated data, “dirty words”, etc. A 100% compliance, pass/fail view should be taken.

5.5.1 Tresys Technology XD Air

The Tresys Technology XD Air product provides state-of-the-art file analysis and filtering technology which:

- Detect virus or malware infected files
- Clean and verify files are cleansed
- Remove unknown file types
- Remove steganography
- Analyze, remove, and cleanse embedded objects
- Remove or cleanse color or size obfuscated text
- Remove macros from documents
- Remove or cleanse metadata
- Remove unrecognized data
- Validate file formats
- Identifies hidden content

5.5.2 Indicate the success or failure within the media tracking system.

5.5.3 Scan Success

Media is available for use (or for next step in current process).

5.5.4 Scan Failure

5.5.4.1 Data Ingress Media

Media that fails the scan should NOT be used on Digital Assets.

5.5.4.2 Data Egress Media

Media that fails the scan which was used on Digital Assets to export data indicates the Digital Asset has been compromised.

5.5.4.3 Contact local security authorities for proper handling of this compromised media. As appropriate, dispose of media (see 6.8).

5.5.5 Exceptions

5.5.5.1 The scanning product used may have the capability to provide controlled and logged exception-handling of data that normally would fail the scanning process. For example, it may be policy that no executables (programs) can be ingress data, but a digital asset can only be updated via a vendor supplied update executable.

5.5.5.2 Though scanning products cannot guarantee an executable is completely safe, they can provide a means of uniquely identifying an executable to permit the exception to that one executable during the scanning process. The process will recognize the executable, log the exemption and pass the scan.

5.5.5.3 This exception handling requires additional process and authentication by local security authorities.

## 5.6 Secure Data Transfer

This process securely transfers data from a particular "source" media to a previously cleaned "destination" media. The process scans and filters source data for local policy and security compliance. This process is a destructive process for the destination media. That is, this process cleans the destination before writing the data.

5.6.1 Obtain source media

The source media can be provided from internal or external sources (ex. a USB from a vendor).

5.6.2 Obtain destination media

Media must be Checked-Out from Media Pool

5.6.3 Initiate Secure Data Transfer following vendor procedure

5.6.4 Review Secure Data Transfer results

5.6.4.1 The resulting files on the destination media have passed the filtering and scanning policies. They may include a mix of

5.6.4.1.1 Unmodified original data files

5.6.4.1.2 Modified original data files (ex. local policy may dictate that meta-data be removed from Office files).

5.6.4.2 Some file will not be transferred, failing to pass the filtering and scanning policies.

5.6.4.3 Based on the results of the transfer to the destination media determine whether to continue with the intended Data Ingress.

## 5.7 Quarantine

The intent of the Quarantine is to physically isolate external media from Digital Assets.

5.7.1 This procedure applies to all external media, whether the media contains data intended or appropriate to Digital Assets.

5.7.2 External media contacting ingress data should have the date securely transferred to clean internal media via a Secure Data Transfer (see 6.6)

5.7.3 Render external media inaccessible. Options include but not limited to
- 5.7.3.1 Locked location
- 5.7.3.2 Tamper-Evident containers or bags

## 5.8 Media disposition

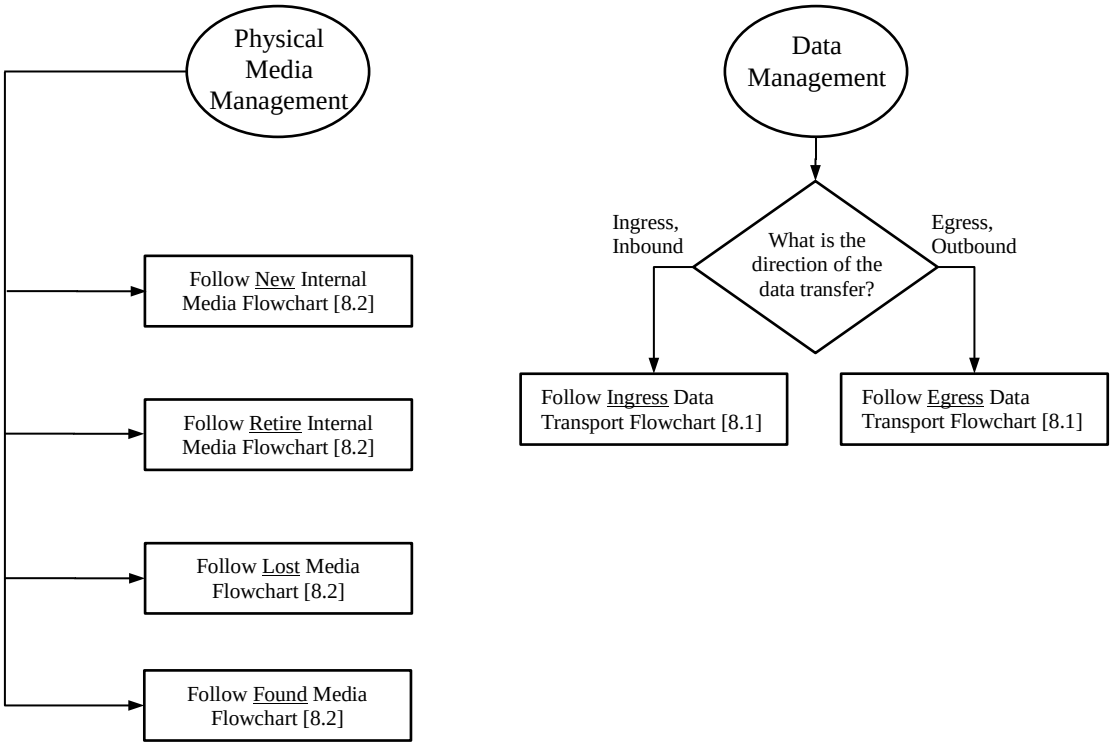
When media can no longer accurately store data, permit the storage of new data (ex. single-use CD-ROMs) or otherwise is deemed unusable, it must be properly disposed of.

5.8.1 External media
- 5.8.1.1 Update media tracking information.
- 5.8.1.2 Return to external entity
- 5.8.1.3 Remove from facility

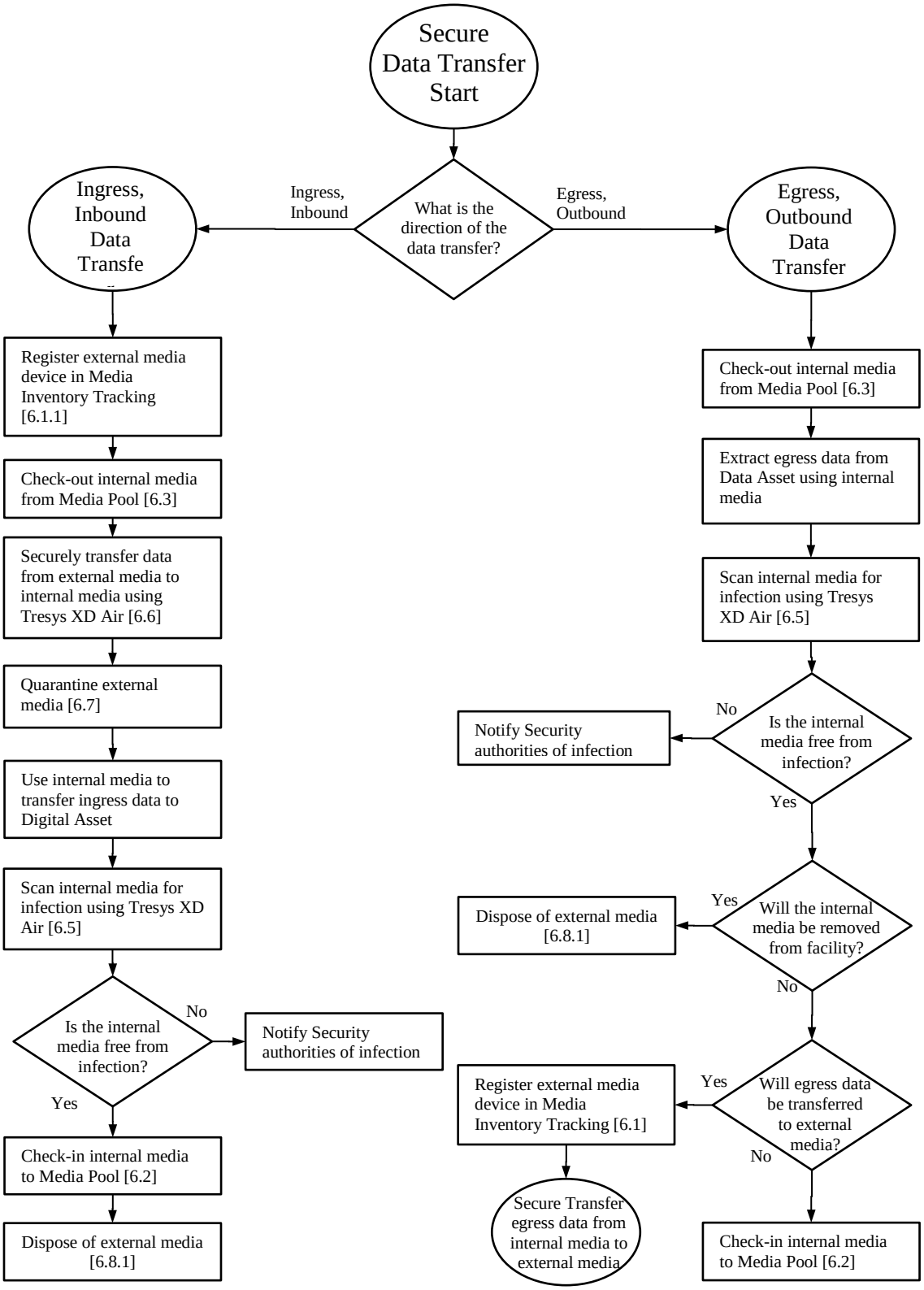
5.8.2 Internal Media to be removed from facility
- 5.8.2.1 Update media tracking information.
- 5.8.2.2 Remove from facility

5.8.3 Aging, failing media
- 5.8.3.1 Update media tracking information.
- 5.8.3.2 Physically dispose or destroy as directed by local policies

# 6 FLOWCHARTS FOR PROCESSES FOR DATA MEDIA MANAGEMENT



## 6.1 Data Transport Flowchart



## 6.2 Media Management