ARKANSAS AIR NATIONAL GUARD
HEADQUARTERS 223rd AIRLIFT WING (ANG)
LITTLE ROCK AIR FORCE BASE ARKANSAS

01 DEC 2020

MEMORANDUM FOR ALL 223rd CYBER OPERATIONS SQUADRON PERSONNEL

FROM: 223rd ISSM\ISSO

SUBJECT: 223rd CYBER OPERATIONS SQUADRON Magnetic Media Responsibilities

PURPOSE: This letter is to educate all personnel on procedures required to handle magnetic media. It applies to all military personnel, civilian government employees, and contractors working at the 223rd CYBER OPERATIONS SQUADRON.

1. General Information:

1.1. Magnetic media refers to any surface used to store electronic data. This includes, but is not limited to: reel-to-reel magnetic tapes, audio/video cassette tapes, data storage cartridges, laptop computers, hard drives, USB drives, CDs, DVDs, floppy disks, and memory flash cards.

1.2. Internal (fixed) computer hard drives will not be controlled under the magnetic media program as they are controlled separately by the unit ADPE custodian.

1.3. Magnetic media can be reused if it will store an equal or higher level classification of data as indicated by the prior classification marking. Classified magnetic media will not be downgraded or declassified.

2. Responsibilities: Information System Security Officers (ISSO) are responsible for the creation and maintenance of all media logs. These locally developed logs will be used to issue, track, & account for all media throughout its life-cycle.

- All magnetic media entering and exiting the SCIF will be coordinated via the ISSO or SSR. The ISSO or SSR will virus scan all CDs/DVDs and ensure they are finalized and properly labeled. All media will be logged on a Media Login Sheet by entering your name, date, contents of the media, type of media, and the date of removal/destruction. The media login sheets are located just inside the SCIF entrance on a clipboard.

- Laptop Computers: In the event that COMM personnel must bring a laptop into the SCIF for trouble shooting or maintenance, the laptop must be checked in via the ISSO. The ISSO will ensure there is no unauthorized software on the laptop and that all wireless capabilities are disabled.

- The Media Control Library binders document each item's unique media control number, classification, type of media, date of issue, storage location, and disposition. All media in the SCIF, regardless of classification, must be assigned a media control number and added to this library. All media in the library will be inventoried annually as a minimum. The media library binders are stored on a shelf in the ISSO/SSR office and are designated by classification (SCI, SECRET, or UNCLASS).

- The Laptop/External HD Sign-Out log is a clip board containing sign out sheets for laptop computers and removable hard drives in the SCIF. It is maintained by the ISSO and the SSR. All laptop computers and removable hard drives are retained in locked containers and controlled by the ISSO. IT and IA personnel can sign out laptops and removable hard drives via the SSR/ISSO as necessary.

- The Magnetic Media Tracking Log is a binder containing sign out sheets for media (other than laptops and hard drives) assigned to the SCIF and is maintained by the ISSO. It will be used to record movement of media outside of its normal storage location. Do not use this log to annotate the introduction or creation of new media or the destruction of existing media; instead use the Media Library binders for these purposes. When media is moved from its storage location, write an entry in the Magnetic Media Tracking Log showing media control number, location, contents, sign out date, your name, and the date when the media is returned.

- Users are the most important entity to ensure proper media security and control. Users with a requirement for media will coordinate with the ISSO or SSR to ensure proper media handling procedures are followed. Users are required to follow all security policies and practices placed in effect by the ISSO and SSR. If a user observes an actual or suspected violation, or if the user has questions or doubt regarding proper security practices, he/she should contact the ISSO immediately.

3. All 223rd CYBER OPERATIONS SQUADRON personnel will:

   - Immediately report the loss of any magnetic media to the unit ISSO or SSR.

   - Turn in media that is no longer needed to the ISSO/SSR for destruction/disposal.

4. Labeling Requirements: All personnel assigned to the SCIF are responsible for proper labeling (using the SF 700-series labels) of all media under their purview. **Every piece of media within the SCIF will be properly labeled.**

   - An SF 711 (Data Descriptor Label) will be affixed to each piece of media containing data with the exception of optical (CD/DVD) media, where the labels will be placed on the casing and the control number written in permanent marker on the CD/DVD (reference JDCSISSS 6.4.1). The media will also have the appropriate Standard Form 700-series classification label. Use the following labels:

UNCLASSIFIED	Green	SF 710
CONFIDENTIAL	Blue	SF 705
SECRET	Red	SF 704
SCI	Yellow	SF 712

- When new media with data already on it is received it shall be opened, assigned a control number, entered into the Media Control Library, and labeled with the SF 711 & SF 700-series classification label. Store the new media by classification in one of the Media Library binders.

- All blank media is controlled by the ISSO/SSR. When a box or package of blank media is opened, all media contained in the box or package becomes a controlled item, and must be stored and controlled in the locked media cabinet located in the ISSO/SSR office.

5. Controlling Media: All media within the SCIF will be controlled & accounted for at all times, regardless of classification. The ultimate responsibility for this lies with the ISSO, but users who choose to have media stored at their desks as opposed to SCIF media library are responsible for control of that media. **No music, video, or personally owned media /software will be introduced to government systems unless procured through official government channels and/or approved by the ISSO or SSR.**

5.1. In the event that unauthorized media is introduced into or found in the SCIF, the ISSO or SSR will confiscate the media immediately. An inquiry will be conducted to determine if the media touched any information systems or recorded any data. The media will be scanned and reviewed by the ISSO to determine if the violation is an actual security incident or an infraction. The review will take place on a Security Stand Alone computer. Based on the review and determination by the ISSO, the media will be retained or released. Depending upon the seriousness of the incident, the individual accountable for introducing the media into the SCIF will be provided remedial training or reprimanded by the ISSM.

5.2. The primary means of control & accountability will be the use of:

- Media Login Sheets
- Magnetic Media Tracking Log
- Laptop//External HD Log
- Media Library - The Media Library is the storage location where the ISSO stores all assigned media. Examples of media normally stored in the Library:
    - Common media used by numerous users which needs a central storage location
    - Application software that is only needed by system technicians or administrators
    - Training media
    - Blank media
    - Any media that is not needed by user on a frequent basis.

6. Media Destruction within the SCIF: Media destruction will be performed by, or supervised by the ISSO or SSR. If a user deems a piece of media no longer of use, please contact the ISSO for destruction. Destruction must be annotated in the disposition column of the Media Library binder by entering the date destroyed.

6.1. The exception to this is for **Top Secret** media. Destruction of this media, along with being documented in the Media Control Log “Date Destroyed” block, will also be documented on an AF IMT 310 (Document Receipt & Destruction Certificate). Two people must be present during destruction of Top Secret media (ref. AFI 31-401, 1 Nov 05, para.5.28.2).

6.2. Classified CDs and DVDs will be destroyed using the SEM 0202 OMD located in room 30. Classified floppy diskettes will be shredded using the SEM 244/4 crosscut shredder located in room 27. Remove diskette cover prior to shredding. All other classified media (tapes, hard drives, flash drives) that are no longer needed will be sent to NSA for destruction. **Note:** Destruction of controlled SCI media will be coordinated with the 223rd CYBER OPERATIONS SQUADRON ISSO/SSR before being conducted.

6.3. Shipment/Release: Personnel shipping or hand carrying magnetic media off Little Rock AFB will:

- Package the media IAW AFM 14-304 and DoD 5105.21-M-1. All classified magnetic tapes and hard drives will be sent via proper channels (DCS or registered mail) and MUST be coordinated through 223rd ISSO/SSR.

- Ensure AF Form 310, Document Receipt and Destruction Certificate is properly prepared and sent with the material destined for off base locations.

7. For all questions concerning magnetic media procedures, please contact the unit ISSO or SSR.

VADEN.CORREDUR.JERRICE.1456650704

Digitally signed by VADEN.CORREDUR.JERRICE.1456650704
Date: 2020.12.01 14:02:29 -06'00'

Corredur J. Vaden, TSgt, AR ANG
ISSO/ISSM, 223rd Cyber Operations Squadron