ANNE ARUNDEL COUNTY DEPARTMENT OF DETENTION FACILITIES ADMINISTRATIVE DIRECTIVE	AD NO: 09.03 DATE: August 15, 2024 SUBJECT: Information Systems TITLE: CJIS Media Protection, Transportation and Disposal FOR PUBLIC RELEASE: Yes

I. Reference: CJISD-ITS-DOC-08140-5.9.1-5.8 (Media Protection)

II. Applicable To: Anne Arundel County Department of Detention Facilities (AACDDF)

III. Purpose: To ensure strict compliance with the Criminal Justice Information Services (CJIS) Security Policy on Media Protection. The AACDDF shall establish and implement policies and procedures that control CJIS media access, dissemination, protection, transportation and disposal of CJIS electronic and physical media.

IV. Policy: It shall be the policy of the AACDDF to provide for management information system access by designated employees trained in system security requirements.

V. Procedure:

A. FBI-CJIS requires agencies to document and implement policies and procedures regarding electronic and physical Criminal Justice Information media, to ensure the following: The agency shall securely store electronic and physical media within physically secure locations or controlled areas and restrict access to authorized individuals. Furthermore, the agency shall protect and control such media during transport outside these controlled areas and restrict activities associated with the transport of such media to authorized personnel. Lastly, agencies shall sanitize and destroy media.

1. That access to electronic and physical media, in all forms, is restricted to authorized individuals.

2. That electronic and physical media be stored in secure locations or controlled areas and restricted to authorized individuals.

3. That electronic and physical media be protected during transport outside controlled areas and the activities of authorized personnel transporting such media be restricted.

4. That electronic and physical media be sanitized prior to disposal or release for reuse and that inoperable media or media that is no longer required, be destroyed, and such destruction is witnessed or carried out by authorized personnel. These procedures shall minimize the risk of sensitive information

compromise by unauthorized individuals. Such destruction shall be accomplished by shredding or incineration.

B. Media Protection

1. The AACDDF shall store all CJIS electronic and physical media within secured locations or controlled areas within county detention facilities. Such areas include those protected by electronic key-access.

2. The AACDDF Superintendent shall designate who is authorized access to the CJIS electronic and physical media.

3. Access to CJIS electronic media shall require a valid user's Anne Arundel County network credential. Network credentials and access levels are controlled by the Anne Arundel County Office of Information Technology. This allows authorized personnel access to county computers, its Intranet network and the internet.

4. The general public shall not be granted access to CJIS electronic or physical media.

5. AACDDF authorized personnel shall not utilize public-use computers to access, process, store or transmit CJIS Information. Public-use computers include, but are not limited to, computers used in:

   a. Hotel Business Centers

   b. Convention Centers

   c. Public Libraries

   d. Public Kiosks

6. Electronic or physical media shall be transported and destroyed in accordance with Section V.D. and Section V.E. of this directive.

7. AACDDF shall store all hardcopy CJIS printouts maintained by Anne Arundel County in a secure area accessible to only those personnel whose job function requires them to handle such documents.

8. If an AACDDF authorized personnel is outside a designated secure area with CJIS electronic or physical media, the AACDDF authorized personnel shall assure that such CJIS information:

   a. Does not leave the authorized personnel's immediate control.

b. CJIS printouts are not left unattended, while physical controls are not in place.

9. Precautions must be taken to obscure CJIS Information from public view.

a. Such as by means of an opaque file folder or envelope for hard copy printouts.

b. For electronic devices like laptops, use session lock use and/or privacy screens.

c. CJIS Information shall not be left in plain public view.

d. When Criminal Justice Information is electronically transmitted outside the boundary of the physically secure location.

i. The data shall be immediately protected using encryption.

10. Lock or log off computer when not in immediate vicinity of work area to protect CJIS Information.

a. Not all personnel have same Criminal Justice Information access permissions and need to keep Criminal Justice Information protected on a need-to-know basis.

NOTE: THIS DIRECTIVE IS NOT TO BE CONSTRUED AS TO LIMIT AACDDF AUTHORIZED PERSONNEL FROM ACCESSING CJIS INFORMATION FROM AUTHORIZED COUNTY-OWNED COMPUTERS THAT ARE SECURELY CONNECTED TO THE COUNTY'S INTRANET NETWORK BY PHYSICAL CONNECTION OR VIRTUAL PRIVATE NETWORK (VPN) THAT MEET CJIS SECURITY PROTOCOLS.

C. Media Dissemination

1. Specific CJIS information is disseminated only on a need-to-know basis.

2. Disseminating CJIS information to another agency is authorized if the other agency is:

a. an Authorized recipient of such information and is being serviced by the AACDDF; or

b. while performing personnel and appointment functions, for Criminal Justice employment applicants.

D. Media Transportation

1. Only AACDDF authorized personnel, designated by the Superintendent, are authorized to transport CJIS electronic and physical media outside of controlled areas.

2. The AACDDF personnel shall protect and control electronic and physical media during transport outside of controlled areas from public disclosure. During transport, they shall restrict their activities while in possession of the CJIS electronic or physical media to pick up/receipt, delivery and/or transfer of such media.

3. While transporting CJIS electronic or physical media between secured locations, the AACDDF authorized personnel shall:

a. properly secure the CJIS electronic or physical media in an AACDDF vehicle.

b. never leave the CJIS electronic or physical media unattended in the vehicle.

c. ensure that Media is not accessible to unauthorized personnel during transport.

E. Media Sanitation and Disposal

1. Any electronic media that contained or contains CJIS information shall not be reused or repurposed. It shall be destroyed by shredding and/or incineration.

2. When CJIS electronic media reaches end of service life, the AACDDF designated personnel(s) shall gather CJIS electronic media throughout the Department.

3. Upon receipt, the authorized personnel(s) shall:

a. segregate CJIS electronic media from non-CJIS electronic media.

b. list CJIS electronic media by serial number on the CJIS Electronic Media Disposal Form.

c. arrange to deliver electronic media to the Anne Arundel County Police Department (AACPD) for disposal/destruction.

d. deliver electronic media to the designated AACPD person(s).

e. on delivery, AACPD recipient shall sign the CJIS Electronic Media Disposal Form.

f. receive notification from the AACPD recipient when destruction is complete.

g. update the CJIS Electronic Media Disposal Form.

h. forward completed CJIS Electronic Media Disposal Forms to the NCIC Audit Coordinator with a copy to the Compliance Office.

4. CJIS physical media shall be securely disposed of when no longer required by shredding or incineration. AACDDF authorized personnel shall properly dispose of CJIS physical media as determined by their immediate supervisor.

5. The immediate supervisor of authorized personnel shall ensure the disposal or destruction is witnessed and carried out by the authorized personnel.

This directive shall be reviewed annually and revised as necessary.

Christopher Klein
Superintendent

Rescinds: AD 09.03 dated July 16, 2015

Appendix 1 – CJIS Electronic Media Disposal Form