

ANNE ARUNDEL COUNTY
DEPARTMENT OF DETENTION FACILITIES

ADMINISTRATIVE DIRECTIVE

AD NO. 09.02
DATE: August 15, 2024
SUBJECT: Information Systems
TITLE: System Security
FOR PUBLIC RELEASE: Yes

- I. Reference: MCCS .01E, .01F, .08A, .08E, .08G; Maryland Automated Identification System (MAFIS); Maryland Enforcement Telecommunications Enforcement Resources System (METERS); National Information Center (NCIC); National Law Enforcement Resources System (NLETS); Motor Vehicle Administration (MVA); Anne Arundel County Office of Information Technology; Anne Arundel County Police Records Management System; Offender Management System (OMS) User Manual; AD 07.01, 07.02, 07.03, 09.01, 09.03
- II. Applicable To: Anne Arundel County Department of Detention Facilities (AACDDF)
- III. Purpose: To establish guidelines for authorizing employee access to management information systems and ensuring system security.
- IV. Policy: It shall be the policy of the AACDDF to provide management information system access by designated employees trained in system security requirements.
- V. Procedure:
- A. Management Information Systems
1. The AACDDF shall operate or have access to a variety of management information systems to include:
 - a. National Crime Information Center (NCIC)
 - b. National Law Enforcement Telecommunications System (NLETS)
 - c. Maryland Automated Fingerprint Identification System (MAFIS)
 - d. Maryland Electronic Telecommunications Enforcement Resources System (METERS)
 - e. Motor Vehicle Administration (MVA)
 - f. BlueCheck
 - g. Criminal Justice Information System (CJIS)
 - h. Offender Management System (OMS)
 - i. Maryland Judiciary Secure Case Search
 - j. Dynamic Imaging PictureLink (biometric identification system)
 - k. Department's Local Area Network (LAN)
 - l. Circuit Court System (MDEC)
 - m. District Court System (COURTS/MDEC)
 - n. ICSolutions The Enforcer

- o. ICSolutions Command Bridge Tablet
- p. Commissary System (Keefe)
- q. Financial Management System
- r. County Time and Attendance System (ADP)
- s. E-mail System (Google/Gmail)
- t. Internet
- u. Equifax
- v. LiveScan
- w. Operative IQ

- 2. New or replacement information systems may only be installed or accessed with the approval of the Superintendent.

B. Management Information System Access

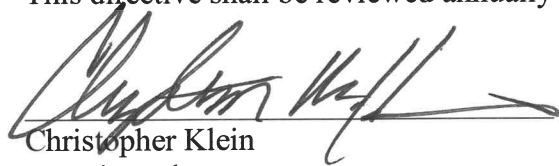
- 1. When an employee is hired, the employee shall be granted authorization to use the management information systems appropriate to their job assignment. This shall occur as part of the Department's initial processing for new employees.
- 2. Supervisors assigned as System Managers shall grant access rights to an employee following:
 - a. Notification of hire date by the Personnel Manager.
 - b. Completion of the New Employee Reception Program.
 - c. Completion of specific management information system training verified or provided by the employee's Supervisor.
- 3. When an employee is reassigned, promoted or leaves County service, the Supervisor shall assign and/or rescind rights as appropriate.

C. Management Information System Training

- 1. Training in the systems shall be provided by:
 - a. NCIC–Maryland State Police (MSP)/Immediate Supervisor
 - b. METERS–MSP
 - c. CJIS–MSP/Immediate Supervisor
 - d. OMS–designated certified training staff or immediate supervisor
 - e. LAN– designated training staff or immediate supervisor
 - f. NLETS, MVA, BlueCheck & MAFIS–Senior Booking Officer and/or their designee
 - g. COURTS/MDEC–designated training staff or immediate supervisor
 - h. Keefe–commissary supervisor
 - i. Financial Management System–immediate supervisor
 - j. County Time and Attendance–immediate supervisor

- k. E-mail–designated training staff or immediate supervisor
 - l. Internet–immediate supervisor
 - m. Equifax–lead Background Investigator
 - n. Dynamic Imaging PictureLink- immediate supervisor
 - o. ICSolutions The Enforcer- immediate supervisor
 - p. ICSolutions Command Bridge Tablet – immediate supervisor
 - q. LiveScan- immediate supervisor
2. The training programs shall include the necessity of maintaining system security to prevent unauthorized access to information as well as the proper use of the information obtained from the systems as it relates to confidentiality and dissemination.
3. Employees requiring access to NCIC shall be certified through MSP and recertified every two (2) years.

This directive shall be reviewed annually and revised as necessary.



Christopher Klein
Superintendent

Rescinds: AD 9.2, dated March 13, 2000
AD 09.02, dated October 15, 2012
AD 09.02 dated January 24, 2023

