Massachusetts Department Of Correction **POLICY**	Effective Date 9/15/2022 Annual Review Date 7/24/2026	Responsible Division Deputy Commissioner, Administration
Policy Name 103 DOC 756 INFORMATION TECHNOLOGY	M.G.L. Reference: M.G.L. Chapter 124, section 1 (c) and (q) DOC Policy Reference: 103 DOC 522 ACA/PREA Standards: 5-ACI-1F-02; 5-ACI-1F-03; 5-ACI-1F-04; 5-ACI-1F-05; 5-ACI-1F-07; 2-CO-1F-01; 2-CO-1F-04; 2-CO-1F-06; 2-CI-2C-1	
Attachments Yes ☒ No ☐ Library Yes ☒ No ☐	Applicability: All DOC Employees/Contract Staff	
Public Access Yes ☒ No ☐	Location: DOC Central Policy File Superintendent/Division Head/Unit Director's Policy File	

PURPOSE:
The purpose is to establish Department of Correction policy and procedure concerning the purchase, acquisition, installation and use of information technology systems (computer hardware, software and related equipment).

RESPONSIBLE STAFF FOR IMPLEMENTATION AND MONITORING OF POLICY:
Deputy Commissioner of Administration
Executive Director of Administration and Finance

CANCELLATION:
This policy cancels all previous Department policy statements, bulletins, directives, orders, notices, rules or regulations concerning information technology systems for Department of Correction facilities, institutions, divisions or units, and employees which are inconsistent with this policy.

SEVERABILITY CLAUSE:
If any article, section, subsection, sentence, clause or phrase of this policy is for any reason held to be unconstitutional, contrary to statute, in excess of the authority of the Commissioner, or otherwise inoperative, such decision shall not affect the validity of any other article, section, subsection, sentence, clause, or phrase of this policy.

TABLE OF CONTENTS

756.01	General Policy	3
756.02	Scope	3
756.03	Ownership	3
756.04	Responsible Staff	4
756.05	Acquisition of Information Systems: Hardware, Software and Related Technologies	4
756.06	Annual Inventory	6
756.07	Authorized Access	6
756.08	Training	9
756.09	Security of Systems	9
756.10	Disaster Recovery	13
756.11	Annual Audit	13
756.12	Strategic Plan	14
756.13	Conformance with Established Administration & Finance Guidelines	14
756.14	Review Date	14

ATTACHMENTS

Attachment #1	Request for Installation of CJIS Terminal	15
Attachment #2	Request for Installation of Non-DOC Hardware/Software	16
Attachment #3	Inventory of Non-DOC Hardware/Software	17
Attachment #4	IMS Profile Approval Procedures	18

756.01 GENERAL POLICY

The Department of Correction acknowledges that people, hardware, software, telecommunications, institutions, and data together form an information technology (IT) system that is highly effective. However, all IT systems involve certain risks that must be addressed through proper controls that assure:

1. Department of Correction IT systems operate effectively and accurately;

2. There are appropriate technical, personnel, administrative, physical, environmental, and telecommunications safeguards in IT systems; and

3. The continuity of the operations of IT systems that support critical agency functions is preserved.

756.02 SCOPE

103 DOC 756 applies to all computing platforms, including local and wide area networks, systems, and applications used to process Department of Correction information. It also applies to users of those systems and applications, including those who install, develop, maintain, administer, and use those systems and applications for the Department of Correction and external entities.

103 DOC 756 applies to all automated technology currently in existence and to any new automated technology acquired or developed after the effective date of 103 DOC 756.

All users of Department of Correction information technology networks and resources shall abide by all applicable Departmental, and State guidelines, policies, regulations, statutes, and procedures pertaining to confidentiality and privacy in accordance with EOTSS IS.000, Enterprise Information Security Policy.

756.03 OWNERSHIP

All Department of Correction data, programs, systems, and procedures (hereafter called "information") gathered, stored, or maintained by the EOPSS-IT, are the property of the Department of Correction, unless otherwise stated in a contractual agreement.

Any person, group, or custodian accessing Department of Correction information must recognize his/her/their responsibility to preserve the security and confidentiality of said information. Such information shall be used only for conducting official business for the Department of Correction. Staff shall utilize such information only in accordance with all applicable provisions of Federal and State statutes and Department of Correction policies, including statutes and policies governing the use

and dissemination of Criminal Offender Record Information (CORI), Evaluative Information, medical record information, substance abuse information and personal data. More specifically, users are prohibited from using their profiles to view data files that are not necessary to the conduct of their normal business, commensurate with their position and role within the organization. Furthermore, staff shall not query data or print file information at the request of others, to provide to others, or to satisfy their own interest or curiosity. Under no circumstances shall an employee share such information with others if it is not in the normal course of his/her/their duties to do so. Additionally, if an employee cannot view information based on his/her/their profiles; they are not authorized to obtain that information in any other manner. The unauthorized querying, printing, or sharing of data or information shall constitute a violation of the employee rules and regulations and may result in disciplinary action.

756.04 RESPONSIBLE STAFF

1. The Deputy Commissioner of Administration shall be responsible for implementing and monitoring this policy throughout the Department.

2. Each Superintendent, Division Head and Unit Director shall be responsible for implementation of this policy at their respective institution, division or unit, and for the development of any and all necessary policies and procedures.

756.05 ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS: HARDWARE, SOFTWARE AND RELATED TECHNOLOGIES`

1. Information technology systems obtained by any Department of Correction institution, division or unit shall follow these general guidelines in accordance with OSD Procurement Policies 801 CMR 21.04:

    a. User - friendliness: The system is easy to use and to learn. Highly specialized training is not required to operate the systems.

    b. Open architecture: The hardware shall allow for the incorporation of features developed by a third party into the original system.

    c. Open systems: The software shall allow for development of new applications by EOPSS/OTIS or other parties.

    d. Connectivity: The systems shall have the ability to interact with local, state and federal information systems, provided that appropriate standards and communication protocols are complied with.

2. All Department institutions, divisions and units shall only purchase or acquire information technology systems hardware, software or related technology that is approved by EOTSS and EOPSS in accordance with OSD Procurement Policies 801 CMR 21.04 and EOTSS Hardware and Software Standards.

3. All information technology systems hardware, software or related technology will be purchased or acquired in coordination with the EOTSS, EOPSS-IT, and/or OTIS (based on requested technology) and the staff of the institution, division or unit funding the procurement in accordance with OSD Procurement Policies 801 CMR 21.04.

4. There shall be a centralized database of the Department's information technology systems, known as the Inventory Tracking Database. This database will be maintained and updated by designated EOTSS staff as a result of such procurement and/or as specified in section 756.06.

5. EOTSS or EOPSS/IT (based on requested technology) shall coordinate with each institution, the delivery and installation of any information technology systems. Installation of Local Area Network servers and all other network hardware shall be at the direction of the EOTSS to ensure that appropriate security and environmental precautions are adhered to in accordance with EOTSS IS.006, Communication and Network Security Standard.

6. EOTSS shall ensure that adequate disaster suppression plans are developed to prevent damage to information technology systems and to detect potential environmental threats (fire, smoke, water, and lightning) in accordance with EOTSS IS.005, Business Continuity and Disaster Recovery. The Superintendent, Division Head, or Unit Director, in consultation with EOTSS, shall ensure that all Local Area Network (LAN) servers and network connectivity equipment are maintained in a secure area of the institution with controlled access, which poses minimal threat of damage to the technology systems and has disaster preventive controls in place in accordance with EOTSS IS.013, Physical and Environmental Security Standards.

7. To ensure an open-system architecture and standardization of Departmental databases, all requests for database development and/or enhancements shall be forwarded to EOPSS-IT Director of Application Development and Support. The Director of Application Development and Support will review these requests to determine application specifications and required development resources. EOPSS-IT will only support development of or enhancements to databases, which have been prioritized by the Department and follow departmental standards of an open-system architecture.

756.06 ANNUAL INVENTORY

1. On or before June 30th of each year, the designated staff of EOTSS along with the appropriate staff of institutions, divisions and units shall conduct an inventory of all information technology systems hardware, software and other related technology in its possession or under its control, and shall update the Department Inventory Tracking Application as needed. The results of the Annual Inventory shall be forwarded to EOTSS through the ServiceNow application for review.

2. Upon the acquisition, transfer, surplus or purchase of any information technology systems hardware, software or related technology the appropriate change(s) shall be entered into the Department Inventory Tracking Application by the designated DeskSide Support technician.

3. If any information technology systems hardware, software or related technology is lost or stolen, the facility, institution, division or unit shall immediately notify EOTSS via submission of a ServiceNow ticket. EOTSS may request a full report concerning the circumstances of the reported loss or theft and may require further investigation if warranted. In such cases all investigations shall adhere to 103 DOC 522, *Professional Standards Unit*.

756.07 AUTHORIZED ACCESS

The intent of this policy is to provide authorized access for personnel, dependent on their job assignment to any information technology system maintained by the Department. To ensure system security and integrity the following guidelines shall be adhered to in accordance with EOTSS IS.006, Communication and Network Security Standards:

1. Wide Area Network (WAN)/Local Area Network (LAN)

    a. Access to the Department's information systems, its institutions and components shall be governed by this policy as administered by EOTSS;

    b. Access to specific applications is regulated by EOTSS and managed by the submission of a ServiceNow ticket on behalf of the Superintendents, Division Heads or Unit Directors;

    c. Any Department employee or vendor may be granted access to the system and its applications, dependent on job assignment and authorization;

    d. Individuals authorized to request new user access to the Department's information systems are limited to Command Staff, Superintendents,

Deputy Superintendents, Division Heads, and Unit Directors. These individuals shall make such requests to EOTSS through the ServiceNow application.

e. Once a username is created, the individual receiving access will determine a password for him/her/them to be used when logging onto the system. **Under no circumstances will this password be shared with any other staff person or individual.** The password devised will remain in effect for a certain amount of time but must be changed by the individual periodically. Passwords are required for information systems and local area network (LAN) access in accordance with EOTSS IS.003 Access Management Standard;

f. **Under no circumstances should any staff member solicit another staff member's password or offer their own.** Contact the designated Department staff member permitted to immediately reset passwords if discovered or revealed. Should no such staff member be available, a ServiceNow ticket should be immediately submitted.;

g. Each institution, division and unit shall develop procedures to ensure access to and to maintain security, and integrity of the local network in accordance with EOTSS IS.003 and IS.006.

2. Inmate Management System (IMS)

Access to modules within the Department's Inmate Management System (IMS) will be granted in accordance with Attachment #4, IMS Profile Approval Procedures. Furthermore, any person, group, or custodian accessing Department of Correction information must recognize his/her/their responsibility to preserve the security and confidentiality of said information. Such information shall be used only for conducting official business for the Department of Correction. Staff shall utilize such information only in accordance with all applicable provisions of Federal and State statutes and Department of Correction policies, including statutes and policies governing the use and dissemination of Criminal Offender Record Information (CORI), Evaluative Information, medical record information, substance abuse information and personal data. More specifically, users are prohibited from using their profiles to view data files that are not necessary to the conduct of their normal business, commensurate with their position and role within the organization. Furthermore, staff shall not query data or print file information at the request of others, to provide to others, or to satisfy their own interest or curiosity. Under no circumstances shall an employee share such information with others if it is not in the normal course of his/her/their duties to do so. Additionally, if an employee cannot view information based on his/her/their profiles, they are not authorized to obtain that information in any other manner. The unauthorized querying, printing or sharing of data or

information shall constitute a violation of the employee rules and regulations and may result in disciplinary action.

3. Criminal Justice Information System (CJIS)

All authorized users of CJIS shall adhere to the official policies and procedures of the Criminal History Systems Board (CHSB) and the signed CJIS User Agreement. Each institution shall appoint CJIS/LEAPS representatives as mandated by the User Agreement.

All requests for the purchase, acquisition, and installation of Criminal Justice Information Systems (CJIS) equipment must be submitted in writing (Attachment #1) via a ServiceNow ticket. . Upon review and approval, the requests will be forwarded to the Department of Criminal Justice Information Services (DCJIS) for processing. All requests for passwords will be made by contacting DCJIS.

4. Security Override

In accordance with the following:

- EOTSS IS.000, Enterprise Information Security
- EOTSS IS.003, Access Management Standard
- EOTSS IS.006, Communication and Network Security Standard
- EOTSS IS.009, Information Security Incident Management Standard
- EOTSS IS.016, Vulnerability Management Standard

If EOTSS Staff detect any activity, which represents a breach of security, they shall have the authority to immediately suspend that person's access to the WAN, LAN and/or all files.

This termination of authorized access and the action(s) which caused it shall be reported to EOPSS-IT's Director of Application Development and Support and Superintendent, Division Head or Unit Director immediately after all access is suspended. The Superintendent, Division Head or Unit Director shall fully investigate this incident and submit a report to EOTSS. The Superintendent, Division Head or Unit Director may request EOTSS to reinstate the person's access based upon the results of the investigation. Reinstatement of authorized access is at the sole discretion of EOTSS. EOTSS will request a ServiceNow ticket be opened and assigned to appropriate staff for reinstatement.

5. No Expectation of Privacy

In Accordance with EOTSS IS.000 Enterprise Information Security Policy and EOTSS IS.002, Acceptable Use of Information Technology, Agency, Board, and Commission computers are the property of the Commonwealth of Massachusetts and are to be used in conformance with state guidelines

for use of information technology resources. In order to ensure proper network operations, Network Administrators routinely monitor network traffic and users should be aware that the Secretariat and its Agencies, Boards, and Commissions, as well as EOTSS, have the right and ability to track Internet sites to which a networked PC connects. The Secretariat and its Agencies, Boards, and Units retain the right to inspect any User's computer, any data stored on it, and any data sent or received by that computer. This right may be exercised at any time. Use of an Agency computer constitutes express consent for the Agency to monitor and/or inspect any data that users create or receive, any message they send or receive, and any web sites they access.

Users should be familiar with the guidelines for E-Mail outlined in state guidelines governing the use of information technology resources and be aware of the fact that Agency, Board, or Unit related E-mails will be subject to the records retention and disclosure requirements of the Public Records Law, unless protected under an applicable exemption or privilege as determined by the keeper of such records.

756.08 TRAINING

The Department, through its Division of Staff Development will ensure that all employees receive adequate training in the understanding and use of all information technology systems that are officially provided or made available to the staff during the course of their duties or job assignments. EOTSS and EOPSS-IT may perform an advisory role in the selection of curriculum and course content for information systems training for Department employees.

Each Superintendent, Division Head, or Unit Director shall ensure personnel under their command are properly trained, by a certified trainer, in the use of any Department computer system.

756.09 SECURITY OF SYSTEMS

1. Guidelines on Staff Use

   EOTSS shall maintain security and integrity of all information technology systems hardware, software and related technology in accordance with the following policies:

   - EOTSS IS.000, Enterprise Information Security
   - EOTSS IS.004, Asset Management
   - ETOSS IS.007, Compliance
   - EOTSS IS.010, Information Security Risk Management
   - EOTSS IS.014, Secure System and Software Lifecycle Management
   - EOTSS IS.016, Vulnerability Management

To lower the risk of IT security violations regarding the use of and the transferring of image and data files to DVDs and CDROMs, the following procedure must be followed:

* Required to reduce the risk of unauthorized use and disclosure of sensitive DVD data
* Process supports and enforces Chain-of-Custody

The DOC Access Control Policy is for Use of Removable Media and Other External Data Collection Devices – Manual Process

A. Create a DVD Workstation Inventory List:

   a. Identify DOC Secured Location of Workstations with External DVDs

   b. Identify External DVD s/n, Make, Model

   c. Identify Laptop s/n External DVD is allocated to

   d. DVD Workstation Inventory List secured by Agency Head w/Agency Head Sign-off

   e. Initial copy of signed DVD Workstation Inventory List to DOC Security Officer and EOPSS CISO for inventory tracking

   f. Quarterly reporting by Agency Head or Delegate to DOC Security Officer and EOPSS CISO for inventory tracking

B. Create a DVD Workstation User Access List

   a. Identify all DOC users of External DVD Workstations

   b. DVD Workstation User Access List secured by Agency Head w/Agency Head Sign-off

   c. Update DVD Workstation User Access List with changes

   d. DVD Workstation User List will be used as a business justification to support access to designated DVD Workstations

C. Secure Laptops and DVDs in a specified location

a. Mount/Secure laptops to workstations in specified secured location identified on DVD Workstation Inventory List

b. Mount/Secure External DVDs to workstations above in the specified secured location identified on the DVD Workstation Inventory List

c. ** Creating a DVD Workstation User Log to identify DVD Workstation use would be of additional benefit to access control

d. Log would identify User, Description of DVD Workstation use, Case/Data accessed and actions

D. Accessing and copying stored DVD Camera Images on Existing DVDs – Using a DVD Reader

a. Using a DVD/Image tool with a DVD Reader, copy/download DVD Camera Images directly from the DVD/Image tool using the DVD Reader to the OneDrive shared folder created for DVD Camera Images only

b. Using a DVD Reader guards against any changes inadvertently being made to the image/data files

E. If downloading DVD Camera Images to a laptop using a DVD/Image tool and a DVD Reader

a. Copy/Download DVD image files to laptop

b. Copy/Upload DVD image files from laptop to the network shared folder created on OneDrive for DOC Camera Images

c. Delete the image file on laptop

d. Destroy DVD

Breaches of security shall be viewed as violations of the established Rules and Regulations of the Department and disciplinary action, up to and including termination may occur for documented violations.

Introduction of unauthorized software, hardware or related technology is prohibited. The introduction of authorized software shall be recorded and catalogued in an official Department Software Library. All copyright

laws and licensing rules shall be adhered to.

Executable files should not be downloaded off the Internet since viruses presently exist in executable files (those files with the .EXE and .COM extensions). However, the newer generation of viruses can live in documents as well. Therefore, without exception, if there is a need to download files off the Internet, EOTSS should be contacted for assistance. Under no circumstances should any file be downloaded unless the file has been checked for viruses using an updated version of anti-virus software in use by the Department. Under no circumstances should files be downloaded regularly or automatically from external servers without the explicit consent of EOTSS or designee. As a general rule, files that are downloaded should not consume more than one megabyte of disk space. Adherence to this guideline will avoid the use of an excessive amount of space on a PC or network hard drive and prevent serious stress to the Commonwealth's connection to the Internet, which is shared by many agencies.

Staff whose responsibilities involve the maintenance and operation of the Department's information technology systems will be allowed to bring into the institution or division such hardware, software and instruments that are necessary for the completion of their task.

Concerning the introduction of any information technology systems hardware, software and related technology by a Department vendor, volunteer or any non-DOC agency or affiliate, proper approval must be granted by the Superintendent or Division Head using Attachment #2. Once completed and signed by the Superintendent or Division Head, Attachment #2 shall be forwarded to EOTSS via a ServiceNow Ticket for final approval.

The Superintendent or Division Head may request the EOTSS or their official representative conduct a security check of this equipment or software entering their respective institution or area.

This security check may include but not be limited to a search for:

a. contraband within computer system;
b. potential threats to the security of the institution;
c. unauthorized software, hardware or other related equipment;
d. illegal activity conducted through the use of computing systems;

Each Superintendent or Division Head may also authorize the security check of any information technology systems hardware, software or related technological equipment exiting their respective jurisdiction.

EOTSS reserves the right to conduct IT security check of the equipment and software entering or exiting any DOC institution.

2. Guidelines on Inmate Use

Inmates are **not allowed any access to any staff associated computing systems, databases, or software**. This includes, but is not limited to, access to the Internet and Department of Correction Intranet. All Department computers and related equipment shall be clearly marked in color-coded labels: **Staff Access Only** or **Inmate Access.**

There are no exceptions.

All non-DOC personnel shall declare in writing (Attachment #2) to the Superintendent or Division Head what information technology systems hardware, software, or related equipment they intend to introduce, for what purpose, and if any inmate will have access. Superintendents, Division Heads, and EOTSS reserve the right to inspect these information technology systems prior to approving them for inmate use.

Each institution, division or unit shall maintain an inventory (Attachment #3) of non-DOC owned information technology systems hardware, software and related equipment introduced to their respective areas, where it is located, for what purpose it is used, and if inmates have access. This inventory shall be forwarded to EOTSS as part of the institution or division annual report specified in Section 756.12.

All Department institutions and divisions shall develop written procedures pursuant to this policy, detailing specific guidelines for their staff to adhere to. Each institution shall also develop written procedures for non-DOC staff to follow, specifically addressing the delivery of any non-Department owned information technology system(s). This includes hardware and software.

756.10 DISASTER RECOVERY

The Department shall maintain a comprehensive reaction plan in the event of a disaster, disorder or emergency in accordance with EOTSS IS.005, Business Continuity and Disaster Recovery Standard.

756.11 ANNUAL AUDIT

Annually, each Department institution, division and unit's information technology systems shall be audited by the Policy Development and Compliance Unit to ensure compliance with technical policies and procedures. It is recommended that this audit process be completed during the official Department or institutional audit cycle.

756.12 STRATEGIC PLAN

The EOPSS SCIO will submit a biennial IT strategic plan to the Commissioner.

756.13 CONFORMANCE WITH ESTABLISHED ADMINISTRATION & FINANCE GUIDELINES

Users are required to understand and follow state and Agency/Board/Commission guidelines governing the use of information technology resources.

756.14 REVIEW DATE

This policy shall be reviewed annually from the effective date by the Commissioner or designee in accordance with 103 DOC 104, *Internal Regulations*.

In the event of a department wide loss of computer infrastructure; a contingency plan for Continuity of Operations Plan (COOP) is located in the Field Services Division Office.

Attachment #1

DEPARTMENT OF CORRECTION
EXECUTIVE OFFICE OF TECHNOLOGY SERVICES AND SECURITY
REQUEST FOR INSTALLATION OF CJIS TERMINAL

Institution/Division: _____ Date: _____

Street address: _____ Local telephone number: _____

Exact location of installation? _____

_____

Approximate distance (measured in feet) to other CJIS terminals at your facility or division?

_____

How many CJIS terminals are located at your facility/division? _____

Please provide the model name, type and serial numbers of all CJIS equipment, including printers:

_____

_____

_____

_____

_____

_____

Who is the facility/division LEAPS/CJIS representative? _____

Have the funds been allocated for this purchase? _____

Do you understand the LEAPS/CJIS User Agreement? _____

Superintendent/Division Head Approval: _____

Date: _____

EOTSS Approval: _____

Date: _____

Attachment #2

DEPARTMENT OF CORRECTION
EXECUTIVE OFFICE OF TECHNOLOGY SERVICES AND SECURITY
REQUEST FOR INSTALLATION

NON-DOC HARDWARE/SOFTWARE

Name of Institution/Facility/Division where equipment/software will be installed:

_____

Vendor Name: _____ Date: _____

Street address: _____

Local telephone number: _____

Inmate will have access? YES NO (please circle one)

Exact location of installation? _____
_____
_____

Reason for installation? _____
_____
_____

Please provide the model name, type and serial numbers of all equipment, including printers and software to be installed: (Attach additional pages as necessary)

_____
_____
_____
_____

EOTSS approval: _____

Date: _____

Attachment #3

DEPARTMENT OF CORRECTION

EXECUTIVE OFFICE OF TECHNOLOGY SERVICES AND SECURITY

INFORMATION TECHNOLOGY INVENTORY

INVENTORY OF NON-DOC HARDWARE/SOFTWARE

Institution/Division: _____ Date: _____

ID Tag Number	Description	Location

Superintendent/Division Head Signature: _____

Date: _____

Attachment #4

Department of Correction

IMS Profile Approval Procedures

1. Each institution shall designate one management level staff person (usually Deputy Superintendent or higher) as the approving authority for profiles.

2. Division Heads shall be the approving authority for Central Office Divisions.

3. All staff requests for profile additions or deletions shall be made to the designated approving authority.

4. If approved, the approving authority shall submit a ServiceNow ticket with the required profiles which will then be assigned accordingly.

5. Institutions may only authorize institution profiles and Division Heads may only authorize Central Office profiles within their divisions (refer to the IMS Profiles documents on the DOC Intranet's IMS page).

6. In all instances when staff transfer, are promoted, or otherwise have a change in job function, the approving authorities should submit a ServiceNow ticket to remove or change the profiles.