COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF CORRECTION

103 DOC 756

POLICY ON INFORMATION TECHNOLOGY SYSTEMS

TABLE OF CONTENTS

MASSACHUSETTS DEPARTMENT OF CORRECTION	DIVISION: Administration
TITLE: Information Technology	Number: 103 DOC 756

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).

References: Massachusetts General Laws, Chapter 124, section 1 (c) and (q).

Applicability: All DOC employees Contract employees. **Public Access**: Yes

Location: DOC Central Policy File/Superintendent's, Division Head's or Unit Director's policy file.

Responsible Staff for implementation and monitoring of policy:
- Deputy Commissioner of Administrative Services Division and CIO

Effective Date: 3/06/2008

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.

756.01 General Policy

The Department of Correction acknowledges that people, hardware, software, telecommunications, facilities, 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 data 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.

756.03 Ownership

All Department of Correction data, programs, systems, and procedures (hereafter called “information”) gathered, stored, or maintained by the Technology Services Division, 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 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 to 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 duties to do so. Additionally, if an employee cannot view information based on his/her 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 the Administrative Services Division and the CIO 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 facility, 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 facility, institution, division or unit shall follow these general guidelines:

   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 in-house program developers 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 facilities, institutions, divisions and units shall only purchase or acquire information technology systems hardware, software or related technology that is approved by the CIO or designee.

3. All information technology systems hardware, software or related technology will be purchased or acquired in coordination with the staff of Technology Services Division and the staff of the facility, institution, division or unit funding the procurement.

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 Technology Services staff as a result of such procurement and/or as specified in section 756.06.

5. The Technology Services Division shall coordinate with each facility 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 Technology Services Division to ensure that appropriate security and environmental precautions are adhered to.

6. The Technology Services Division 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). The Superintendent, Division Head, or Unit Director, in consultation with the Technology Services Division, shall ensure that all Local Area Network (LAN) servers and network connectivity equipment are maintained in a secure area of the facility with controlled access, which poses minimal threat of damage to the technology systems and has disaster preventive controls in place.

7. To ensure an open-system architecture and standardization of Departmental databases, all requests for database development and/or enhancements shall be forwarded to the CIO. The CIO will review these requests to determine application specifications and required development resources. The Technology Services Division 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 Technology Services Division along with the appropriate staff of facilities, 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 the CIO 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 Tech Liaison.

3. If any information technology systems hardware, software or related technology is lost or stolen, the facility, institution, division or unit shall immediately notify the CIO. The CIO 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 518 Investigations Policy.

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:

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

   a) Access to the Department's information systems, its facilities and components shall be governed by this policy as administered by the CIO;

   b) Access to specific applications is regulated by the CIO and managed by the Help Desk 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 through the Technology Services Help Desk using E-mail. Only requests received through E-mail will be responded to;

e) Once a username is created, the individual receiving access will determine a password for his or herself 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;

f) **Under no circumstances should any staff member solicit another staff member's password or offer their own.** Contact the Help Desk immediately to reset passwords if discovered or revealed;

g) Each facility, institution, division and unit shall develop procedures to ensure access to and to maintain security, and integrity of the local network.

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 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 to 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 duties to do so. Additionally, if an employee cannot view information based on his/her 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 facility 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) to the CIO. Upon review and approval the requests will be forwarded to the Criminal History Systems Board (CHSB) for processing.

All requests for passwords will be made through the Technology Services Help Desk via E-mail. Only requests received via E-mail will be responded to.

4. Security Override

If Technology Services 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 the CIO 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 the CIO. The Superintendent, Division Head or Unit Director may request the CIO to reinstate the person's access based upon the results of the investigation. Reinstatement of authorized access is at the sole discretion of the CIO. The CIO will request a Help Desk ticket be opened and assigned to appropriate staff for reinstatement.

5. No Expectation of Privacy

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 the Information Technology Division (ITD), 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 Technology Services Division and 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. The Technology Services Division shall 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

   The Technology Services Division shall maintain security and integrity of all information technology systems hardware, software and related technology.

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, the Technology Services Division Help Desk 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 the CIO 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 the CIO or designee for final approval.

The Superintendent or Division Head may request the Technology Services Division or their official representative conduct a security check of this equipment or software entering their respective facility 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 facility or 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.

The CIO reserves the right to conduct IT security check of the equipment and software entering or exiting any DOC facility.

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 the CIO reserve the right to inspect these information technology systems prior to approving them for inmate use.

Each facility, 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 the CIO as part of the institution’s or division’s annual report specified in Section 756.12.

All Department institutions, facilities and divisions shall develop written procedures pursuant to this policy, detailing specific guidelines for their staff to adhere to. Each facility 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 through the Technology Services Division shall maintain a comprehensive reaction plan in the event of a disaster, disorder or emergency. This shall include detailed plans for the Department's Wide Area Network and all Local Area Networks.

A plan shall be developed identifying specific off-site storage facilities for Local Area Network server tape back-ups.

756.11 Annual Audit

Annually, each Department facility, 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 Annual Report

A) The CIO will submit an annual report to the Commissioner, detailing the status of information technology initiatives.

B) The Superintendent and/or Division Head will prepare an annual evaluation of the information systems housed in their facility. The evaluation shall include a statement as to the effectiveness of all systems as it relates to institutional management. This report will site problem areas and requests for future enhancements and will be submitted annually to the CIO of Technology Services.

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. The party or parties conducting the review shall develop a memorandum to the Commissioner with a copy to the Central Policy File indicating the review has been

completed. Recommendations for revisions, additions or deletions will be included.

103 DOC 756 - ATTACHMENT 1
DEPARTMENT OF CORRECTION
TECHNOLOGY SERVICES DIVISION
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: _____

CIO or designee Approval: _____

Date: _____

103 DOC 756 - ATTACHMENT 2
DEPARTMENT OF CORRECTION
TECHNOLOGY SERVICES DIVISION
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)

_____

CIO or designee approval: _____

Date: _____

103 DOC 756 - **ATTACHMENT 3**

DEPARTMENT OF CORRECTION
TECHNOLOGY SERVICES DIVISION
INFORMATION TECHNOLOGY INVENTORY

INVENTORY OF NON DOC HARDWARE/SOFTWARE

Institution/Division:
Date: _____

ID Tag Number	Description	Location

Superintendent/Division Head **Signature:** _____

Date:_____

103 DOC 756 - 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 notify the Help Desk of the required profiles and the Help Desk shall make the necessary arrangements for the assignments.

5. Institutions may only authorize institution profiles and Division Heads may only authorize Central Office profiles within their divisions (see attachment 5).

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

Institution and Central Office Profiles

Institution Profiles	Central Office Profiles
Administrative I	Administrative I **
Administrative II *	Administrative III *
Admissions/Departures I	Administrative IV *
Admissions/Departures II	Capital Management Division *
Basic Security	Central Classification I *
Classification I	Central Classification II *
Classification II	Central Classification III *
Classification III	Central Investigation *
Closed	Central Records I *
Community Release I	Central Records II *
Community Release II	Comm. Corrections Unit I *
Criminal Records Processing	Comm. Corrections Unit II *
Date Computation I	Complete Restriction on Inmate *
Date Computation II *	Data Collection *
Disciplinary *	Date Computation Division *
D-Hearing Officer *	Department Grievance Coordinator *
DNA Coordinator	Director of Discipline *
DNA Liaison	Disciplinary Reg. Sup.
Education	DNA Central *
Food Services	DNA Coordinator**
Global *	Education Division *
Grievance Coordinator *	Health Services Division *
Housing Assignment	INS *
INS *	Limited Access **
IPS *	Parole *
IPS Restriction on Inmate	Program Assessments **
Inmate Accounts *	Program Division *
Inner Control I	Re-entry Supervisor *
Inner Control II	RRC *
Limited Access	Sex Offender Coordinator – Central *
Limited Restriction on Inmate	State Transportation *
Limited Schedule *	Support Services *
Mail/Property	Victim Services *
Medical ***	
Mental Health ***	
Parole *	
Payroll Authorizer	
Program Assessments	
Programs I	
Programs II	
Property Office	
Re entry	

Records I Records II Records III ***** Release Coordinator Sex Offender Coordinator Sex Offender Treatment Shift Commander SORB Substance Abuse CCU Substance Abuse I Substance Abuse II Transfer Coordinator Trips Unit Operations I Unit Operations II View Inmate Balance Work Assignment Work Supervisor	* Denotes profiles with DOC wide access ** Denotes DOC wide access only when profile is assigned to central office personnel *** May only be assigned to the contracted medical provider staff