STATE OF NEW YORK DEPARTMENT OF CORRECTIONS AND COMMUNITY SUPERVISION **DIRECTIVE**	TITLE **Information Security Policy**		NO. 2810 DATE 09/02/2014
SUPERSEDES DIR# 2810 Dtd. 01/05/2012	DISTRIBUTION A	PAGES PAGE 1 OF 14	DATE LAST REVISED
REFERENCES (Include but are not limited to)	APPROVING AUTHORITY		

I. PURPOSE: To set forth procedures for the implementation and maintenance of controls to protect the confidentiality, integrity, and availability of the Department's information assets and computer infrastructure and to define specific controls necessary to support that purpose within the Department's unique operating environment.

II. POLICY: The Department of Corrections and Community Supervision (DOCCS) computer resources must be restricted from unauthorized access and used in a manner that is consistent with DOCCS security policies and procedures citied herein, and the New York State Office of Cyber Security (OCS) and the New York State Office of Information Technology Services (ITS) security requirements and, wherever practical, industry best practice standards. DOCCS computer resources may be used solely in the conduct of official Departmental business except for incidental personal use that do not conflict with the proper exercise of the duties of the State employee.

Pursuant to Governor Cuomo's Executive Order No. 2, "Review, Continuation and Expiration of Prior Executive Orders," one of the Executive Orders issued by former Governor David A. Patterson that is being continued is Executive Order No. 7, issued June 18, 2008 ("Prohibition against Personal Use of State Property and Campaign Contributions to the Governor"). Employees should make themselves familiar with this mandate, in particular, the Section pertaining to the personal use of State property as contained in Section B, "Prohibition Against the Personal Use of State Property;" paragraph (d), which states: "*State computers shall be used only for official business, except that State computers may be used for incidental and necessary personal purposes, such as sending personal electronic messages, provided that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the State employee."* This is available at "www.ny.gov/governor," through the Executive Orders link.

All DOCCS physical locations must have a designated Computer Security Coordinator (CSC) and Data Processing Liaison (DPL).

The requirements contained herein shall be maintained and updated as necessary, and as determined by the DOCCS Information Security Officer (ISO), to ensure consistency with the above standards, guidelines, and practices as well as applicable regulatory requirements.

III. APPLICABILITY: The provisions of this directive are applicable to all DOCCS computer resources and all personnel using those resources.

IV. SECURITY

A. Asset Management

1. All requests for new, replacement, or additional IT equipment or software including surplus or donated items must follow the DOCCS standard process, including the use of the E-Form #MIS106 as detailed in Directive #2822, "Request for Information Technology Hardware Acquisition/Relocation/Removal." Questions concerning that process should be directed to the designated CSC or the ITS Public Safety Contact Center.

2. All computer data storage media (e.g., tapes, disks, diskettes, cartridges, cassettes, USB drives, etc.) shall be "sanitized" and all data permanently erased and cleared prior to being repurposed and reissued within DOCCS.
3. The correctional facility, Central Office, or other DOCCS location DPL or designee will ensure that proper inventory records of all software and computer equipment are kept in a secure manner. A copy of inventory records will be maintained by each facility, with a copy provided to ITS at least annually. All inventory policies are governed by and detailed in DOCCS Directive #2944, "Equipment Control," and DOCCS Directive #2948, "Reporting Loss of Issued Items."
4. Facility computer equipment shall be relocated only after written permission is obtained from ITS through the E-Form #MIS106. Notification of the move of any microcomputer equipment shall be recorded on the *Personal Computer Equipment Inventory Form*, found in the Facility *Data Processing Liaison Manual* and forwarded to the facility Business Office for local inventory control. Central Office and other DOCCS location relocation requests must be forwarded to the ITS Public Safety Contact Center.
5. Only Information Technology (IT) equipment, including computers, network devices, software, etc., that has been approved via the E-Form #MIS106 process and will be supported by ITS shall be deployed. All requests for hardware and software must be approved by ITS prior to purchase.
6. Absolutely no personal software is to be installed on Department owned equipment. This includes, but is not limited to, screen savers, calendars, instant messaging clients, Internet Service Provider (ISP) software, file sharing programs, etc.
7. Only properly licensed software that has been authorized by ITS may be installed.
8. Security testing software, including sniffers, scanners, and vulnerability assessment tools may not be installed on Department owned computer equipment unless specifically authorized by the ISO.
9. All original software media diskettes, CD's, etc. and software licenses must be forwarded to the DPL in the facilities or, if in Central Office or other DOCCS location, to the ITS Public Safety Contact Center.
10. No programs or applications are to be developed and placed into production without the written approval of ITS as detailed by DOCCS Directive #2821, "Requesting Applications Modification/New Development."

B. Physical Security

1. Equipment should be locked in a secure area when unattended or when visual security of the area cannot be maintained by authorized staff.
2. All computer equipment must be located in work areas or rooms having a limited number of entrances that can be securely locked after normal working hours. These work areas must provide adequate physical protection of the computer resources of the Department against unauthorized use, theft, sabotage, and natural or man-made disasters.
3. Computer terminals and workstations must be positioned to prevent viewing by unauthorized individuals, wherever practical.
4. All computer equipment must be located off the floor, on a desk, table, or workstation. This includes PC tower units.

C. Laptop and Portable Computer Equipment

1. All Department issued portable computers must be configured to provide complete hard disk encryption using cryptographic methods authorized by the ISO.
2. All portable computer equipment must be physically secured when not in use to prevent theft and/or unauthorized access.

D. Configuration Management

1. All computers and network appliances must be configured, administered, and maintained according to DOCCS standard configuration and DOCCS information security policies, as approved by the ISO.
2. All computer terminal and workstations must be configured with screen locks that activate after 15 minutes of user inactivity and must require a password to unlock.
3. All computer, server, and network equipment logon screens must include a legal warning banner containing language approved by the ISO and Counsel's Office.

E. Computer Storage Media Protection

1. Removable electronic media used for the storage of DOCCS data (except media used for routine data back-up and stored in a specific, secured back-up media site) must be encrypted when leaving a secure location. All encryption will use a cryptographic method approved by the ISO.
2. All electronic media used for storage of DOCCS data must be appropriately labeled to reflect its sensitivity and access restrictions. Labeling must include a description of the media contents, date, and owner.
3. All removable electronic media, computer memory, and computer equipment used for storage of DOCCS data must be disposed of in a manner consistent with DOCCS standard practices, including the use of an outside service provider certified by the National Association for Information Destruction (NAID) and/or R2/RIOS.
4. Electronic removable media that contains the personally identifiable protected health information of DOCCS inmates or parolees is considered a "Confidential Health Record" and shall be stored, encrypted, and moved consistent with HIPAA privacy and security regulations and Health Services Policy (this applies to digital copies of x-rays and similar examinations stored on disks).

F. User Identification, User Access, and Passwords

1. All DOCCS computer systems and applications require the use of an authorized user identifier (User ID) and password to gain access.
2. The individual requesting access to DOCCS computer systems must follow the standard ITS Access Request and Approval procedure, including the completion of the Individual User Access (IUA) form, and Form #MIS104 if Internet access is required.
3. ITS shall assign a unique User ID to DOCCS personnel and other authorized individuals requiring access to systems and applications.
4. Individuals requiring privileged access (i.e., Administrator access) to a DOCCS computer, terminal, or network equipment are required to notify the ISO and/or ITS. The ISO and/or ITS will ensure that the level of access granted to the individual is the minimum level required to perform the required job function as specified by the system owner.
5. Users are responsible for all work completed using their User ID and password. Therefore, all passwords should be kept confidential and not shared or divulged to unauthorized personnel. All users should ensure password security by not openly displaying passwords or storing written passwords in easily accessible areas.
6. User IDs and passwords may not be programmed into keyboard function keys or otherwise stored and/or automated.
7. Passwords should be randomly selected and not obvious. Passwords must not be variations of a user's name, birthday, or other specific characteristics that readily identify the operator or the work area.
8. Passwords must be changed at least every 30 days and cannot be reused within 12 months.

9. Passwords must be at least eight characters in length and contain a combination of numbers, upper or lower case letters, and/or special characters.
10. Application owners and/or designated CSCs must conduct annual reviews of all access lists to identify user accounts with access that is not commensurate with the user's current job assignment.
11. The Division Head or designee shall promptly notify ITS via an e-mail to doccs.sm.AAS@doccs.ny.gov when the following events occur:
    a. A user is no longer assigned to the facility; or
    b. A user changes assignments that would affect access authorizations.
12. The Division Head or designee and/or designated CSC shall contact the ITS Public Safety Contact Center in the event a user, administrator, or system password is compromised or reasonably believed to be compromised.
13. The Information Security Office, as directed by the ISO, shall conduct periodic audits to determine the effectiveness and integrity of User IDs and passwords.
14. Access to computer equipment on other than normally assigned work schedules, for special purposes, or on an overtime basis should have the prior approval of the individual's supervisor and a documented copy of that approval provided to, and archived by, the CSC.

G. Document Security

1. Instruction manuals, operating instructions, diagrams, and other sensitive information must not be left unattended, and must be secured and controlled at all times. Inmates must not be allowed access to sensitive documents unless specifically authorized by the Facility Superintendent and Regional Director.
2. Hard copies of personally identifiable information (PII) and protected health information (PHI) must not be left unattended or in view of unauthorized individuals.
3. All computer generated reports must have adequate controls and procedures established to ensure proper filing, distribution, reproduction, mailing, and destruction. DOCCS Directive #2011, "Disposition of Departmental Records," should be consulted for specific details.

H. Secure Operations

1. Users must ensure that unattended computer and/or equipment terminal screens are not left displaying data or allowing access or modification of Department records.
2. Data files obtained from non-Department-owned and controlled computers must be screened for viruses and other "malware" using an authorized software program that has been approved by the ISO according to the DOCCS Antivirus Policy.
3. Those employees that are authorized to perform DOCCS business remotely (i.e., at home or out of the office) must ensure that DOCCS data is protected at all times. It is the responsibility of the employee to be aware of the risks associated with connecting remotely and how remote connections can affect the DOCCS network. All DOCCS issued laptops and other hardware is the responsibility of the employee. For further information regarding remote connection concerns, please contact the Information Security Office.

I. Wireless Communication/Networking

1. The use of wireless voice communications is governed by DOCCS Directive #2917, "Cellular Telephones and Pagers."

2. Wireless data networking equipment is prohibited in all DOCCS facilities and locations, including but not limited to:

    a. Wireless Peripherals: Wireless computer mice, keyboards, printers, scanners, fax, etc.; and
    b. Wireless Networking Equipment: Wireless routers, access points, antennae.

Note: The use of wireless enabled laptops is prohibited as documented by Section IV-C above.

J. Separation of Duties/Audit

1. DOCCS locations should protect themselves from acts of fraud and/or collusion through the strict separation of duties, job rotation, separation of operational and security functions, and system access controls. Security Audits will be conducted according to DOCCS standard *Information Security Audit Procedures* to ensure DOCCS personnel are not auditing their own work. Further information can be found in DOCCS Directive #6920, "Internal Controls."

V. ROLES AND RESPONSIBILITIES

A. Computer Security Coordinator (CSC): The general responsibilities of the CSC are to:

1. Provide liaison with the Information Security Office in matters on computer security and access control.
2. Inform facility/unit personnel of DOCCS computer security policies and standards.
3. Serve as the facility level review and approval authority regarding computer related security matters.
4. Establish controls and procedures for implementing computer security measures.
5. Resolve issues with regard to shared computer resources among different organizational units.
6. Conduct periodic reviews to monitor and evaluate the facility computer security.
7. Assist the Information Security Office with facility level audits and inspections as requested by the ISO.
8. Implement all computer security provisions and initiate corrective actions.
9. Report any breach of computer security to the Superintendent or Regional Director and the ISO.
10. Maintain accurate records of personnel authorizations.
11. Conduct audits, at a minimum annually, based on listing of all users and their authorizations which will be provided by ITS. The CSC shall:

    a. Require each employee with a user identification code and their supervisor verify and attest to the appropriateness of the employee's access (a list of active User IDs for a particular facility should be requested from ITS ISO prior to the annual facility audit);
    b. Provide each employee with a user identification code**,** a copy of this directive, and obtain a receipt;
    c. Provide the ISO with a list of changes and deletions based on the audit findings; and
    d. Retain these documents as a permanent record of the audit review.

12. Review the equipment, its configuration, and the practices in place regarding the use of equipment provided for an inmate training program to verify compliance with this directive.
13. Obtain from the staff advisor of an inmate organization a list of all authorized users for equipment used by that organization. The CSC may access that equipment at any time. If passwords are used or any unapproved software is found on the equipment, the CSC may cause the equipment to be removed immediately.

B. Data Processing Liaison (DPL) The general responsibilities of the DPL are:

1. Provide liaison with the ITS Public Safety Contact Center.
2. Provide the initial problem determination for computer hardware with the guidance and support of ITS and equipment vendors.
3. Provide first level support in the use of e-mail and selected applications.
4. Coordinate requests sent to ITS for terminals, network appliances, printers, emulation boards using the procedures outlined in Directive #2822, "Request for Information Technology Hardware Acquisition/Relocation/Removal."
5. Coordinate, submit, and verify change/add requests for local prints (screen prints). Requests will come from DPL by e-mail to the Public Safety Contact Center.
6. Assist in equipment placement decisions.
7. Field all help and service calls within the facility and determine appropriate action.
8. Maintain computer equipment inventory. This includes but is not limited to laptop computers turned over to the facility as part of contract necessary to monitor, operate, or adjust equipment.
9. Facility staff responsible for computer equipment used for inmate training shall maintain and provide to the DPL an inventory of all equipment and a description of any networking of that equipment.
10. Provide virus-checking on all storage media brought in from outside the facility.
11. Assist in training facility personnel in the proper use of Department computer equipment.
12. Inform the Public Safety Contact Center when a generator test is scheduled.
13. Read e-mail and SYSM bulletin board regularly.

C. Information Technology Assistant (ITA): The ITA is a full-time staff person who reports directly to ITS and is the primary contact for designated DPLs in matters pertaining to computer terminals, network appliances, printers, modems, personal computers, and other related hardware and software. ITAs may be assigned to an individual facility or to a Hub.

D. Information Security Officer (ISO): The ISO and back-up ISO are designated by the Commissioner and report to the Assistant Commissioner for ITS. The ISO ensures that information security policies and procedures are established and implemented to protect the information assets of DOCCS, participates in the creation and review of the policies and procedures, recommends security strategies, and keeps information security systems current. The ISO will ensure that there are procedures in place to prevent, detect, contain, and recover from information security breaches from both internal and external sources and disasters both natural and man-made.

VI. SECURITY VIOLATIONS/INCIDENTS

Any actual or suspected cases of unauthorized use, misuse of DOCCS computer resources, breaches of security, or unauthorized disclosure shall be reported immediately by telephone to the **ITS Public Safety Contact Center** at **518-457-5017.**

The ITS Public Safety Contact Center will report all such calls to the Information Security Office in accordance with the DOCCS *Cyber-Incident Reporting and Response Procedure*.

The ISO will implement an incident containment and response plan in accordance with the DOCCS *Cyber-Incident Reporting and Response Procedure*.

VII. INTRANET/INTERNET ACCEPTABLE USE POLICY

A. Introduction: The Agency connection to the global Internet only exists to facilitate the official work of DOCCS. The Internet facilities and service contributes broadly to the mission of the Department.

The Internet connection and services are provided only for personnel legitimately affiliated with the Department for the efficient exchange of information and the completion of assigned responsibilities consistent with the Department's statutory purposes.

Use of the Internet facilities by any employee or other person must be requested and approved in accordance with ITS E-Form #MIS104. This is the standard ITS Access Request and Approval Procedure and must be consistent with this Acceptable Use Policy and security policies. Questions concerning that process should be directed to the CSC.

B. Principles of Acceptable Use: DOCCS Internet users are required to:

1. Respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other users, unless explicit permission to do so has been obtained.
2. Respect the legal protection provided to programs and data by copyright and license.
3. Protect data from unauthorized use or disclosure as required by State laws, Federal laws, and Agency Regulations.
4. Respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
5. Report any observations of attempted security violations.

C. Unacceptable Use: It is not acceptable to use New York State Internet facilities, or any other Internet connectivity provided by DOCCS:

1. For activities unrelated to the Department's mission and business, except for incidental personal use that does not conflict with the proper exercise of State business, in accordance with Executive Order No. 1, *Establishment of Ethical Conduct Guidelines*,
2. For activities unrelated to official assignments and/or job responsibilities,
3. For any illegal purpose,
4. To knowingly transmit/receive threatening, profane, or harassing materials or correspondence,
5. For unauthorized distribution of NYS data and information,
6. To interfere with or disrupt network users, services, or equipment,
7. To engage in network monitoring, scanning, sniffing, spoofing, or other activities intended to identify, test, or circumvent security controls, unless specially authorized by the ISO,
8. To download, upload, or exchange music or video files without specific authorization by the ISO,
9. To download, upload, or exchange commercial, freeware, or shareware software that has not been approved by the ISO,
10. For electronic messaging including instant messaging (IM) and Internet e-mail that has not been explicitly approved by the ISO,
11. To download, upload, or transmit sexually explicit, violent, or otherwise offensive material,
12. To upload or post information of any kind to web sites, chat rooms, listservs, forums, or other Internet spaces without specific approval by the ISO,
13. For private purposes such as marketing or business transactions,
14. For solicitation for religious and political causes,

15. For unauthorized not-for-profit business activities,
16. For any Union activity,
17. For private advertising of products or services, or
18. For any activity meant to foster personal gain.

D. Agency Rights: DOCCS personnel should have no expectation of privacy relative to the use of DOCCS systems and applications, including electronic messaging. Authorized personnel, including staff of the Information Security Office, have access to all electronic communications and may monitor messages as necessary to assure efficient performance and appropriate use, subject to the approval of the DOCCS Chief Information Officer. Messages relating to, or in support of, illegal activities will be reported to the appropriate authorities.

The Department reserves the right to monitor and log all system and network activity and to inspect any and all files created or modified by DOCCS personnel.

The Department reserves the right to remove a user account from the network.

The Department reserves the right to change its policies and rules at any time. The Agency makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a user outside New York State or any costs or charges incurred as a result of seeking or accepting such advice.
- Any costs, liabilities, or damages caused by the way the user chooses to use his/her Agency Internet access.
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Department. The Department's Internet services are provided on an as is, as available basis.

E. Enforcement and Violations

1. This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet facilities but is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be addressed to the ISO. Other questions about appropriate use should be directed to your Supervisor.
2. This Department will review alleged violations of the Internet Acceptable Use Policy on a case-by-case basis. Violations of the policy which are not promptly remedied may result in termination of Internet services for the person(s) at fault, and referral for disciplinary or legal actions as appropriate.

F. Exceptions

1. Exceptions to this and other DOCCS policies and procedures must be submitted, in writing, to the ISO. The ISO will review and document all exceptions in a manner consistent with *New York State Office of Cyber Security (OCS)* and the *New York State Chief Information Officer (CIO)/New York State Office of Information Technology Services (ITS)*.
2. All exceptions to this and other DOCCS security policies and procedures will be documented, reviewed, approved, and archived by the ISO for a period consistent with applicable retention policies.

G. Additional Restrictions Inside DOCCS Correctional Facilities (Staff)

1. Absolutely no computer equipment, hardware components, or any equipment used for the processing of information that connects or can connect wirelessly to its data source and can be easily moved without extra assistance may be brought into a correctional facility unless authorized by the Facility Superintendent or the ISO. This includes, but is not limited to: tablet, smart phones, blackberries, laptops, and netbook.
    a. No media or device that is capable of storing electronic data (e.g., CDROM, USB drive, diskette, MP3 player/iPOD®, etc.) may be brought into, or removed from, a correctional facility without written authorization by the ISO and/or Superintendent.
2. The following guidelines are applicable to all Department issued or officially approved computer equipment as designated in Section VII-G-1 above:
    a. All portable computer equipment must be physically secured when not in use to prevent theft and/or unauthorized access. All portable computers will be considered a Class "A" tool and must be stored in a Class "A" tool cabinet or in the arsenal as determined and approved by the Superintendent.
    b. All electronic removable media (e.g., tapes, disks, diskettes, cartridges, cassettes, USB drives, etc.) are to be considered Class "A" tools and secured when not in use and/or at the close of business. Class "A" tools are to be stored in approved locations as determined and approved by the Superintendent.
    c. All drives/ports used with removable media (such as floppy disks, CDs, DVDs, USB drives, etc.) will be disabled within a facility. The designated DPL/CSC may enable these drives/ports upon written approval from the Superintendent and the ISO.
3. There are additional guidelines governing various categories of outside State Agency staff, Court Stenographers, visiting Departmental staff, outside vendor staff, or contracted service personnel who may be approved to enter a correctional facility. All staff should familiarize themselves with Deputy Commissioner Bellnier's All Superintendent's memorandum, dated December 8, 2011, regarding laptop/mobile computers in facilities. A copy of this memorandum is included in this directive as Attachment A.
4. All portable computers turned over to facilities as part of contracts and necessary to monitor, operate, repair, or adjust equipment will be turned over to the DPL in accordance with DOCCS Directive #2822. The DPL will register, inventory, and configure the device according to DOCCS standards.

H. Additional Restrictions Inmates

1. Inmate access to computer systems will be strictly controlled as to not allow access to any data network that is logically connected to the DOCCS production network and/or any other externally connected data network. The following are cases in which inmates may access computer systems pending Superintendent approval:
    a. Authorized use of the Inmate Network (Law Library, etc);
    b. Authorized inmate training and/or educational activities; and
    c. Authorized inmate assistance in data entry for non-sensitive data, including Corcraft systems. New York State law states that the Department can not, "Knowingly use the labor or time of or employ any inmate in this State, or in any other jurisdiction, in any capacity that involves obtaining access to, collecting or processing social security account numbers of other individual."

    To request authorization, a written request should be presented by the designated CSC and submitted to the Superintendent for approval.

2. At no time may an inmate have in his/her personal possession any computer storage media outside of his/her assigned classroom or work area. These items will be retained in the classroom or work area under the same provisions used for class "A" tool control.
3. Proof of purchase or proper authorization for all software in use is required for any PC used by an inmate organization. This proof shall be provided to the CSC. Any software proposed for this equipment must be reviewed for content and approved by the facility Superintendent and the ISO.
4. The staff advisor of an inmate organization shall provide the CSC with a list of all authorized users for equipment used by that organization. The CSC may access that equipment at any time.

VIII. DEFINITIONS

A listing of terms defined for the first time in this policy are:

Authentication Confirming a user's claim of identity. Dual factor (or strong authentication): An authentication scheme using two independent factors, e.g., something you know and something you have. Examples include the following:

- Something you know: User ID, passcode, memorized personal identification number (PIN) or password.
- Something you have: something you own- an RSA secure authentication token, Smart card, etc.
- Something you are: biometrics, e.g., fingerprint, retina scan.

Availability "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of ***availability*** is the disruption of access to, or use of, information or an information system.

Business Owner Person who authorized the project, or a designated employee.

Confidentiality "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.

Control An action taken to enhance the likelihood that established goals or objectives will be achieved (in the context of this policy, generally an action taken to reduce ***risk***).

Credential An object that is verified when presented to the verifier in an authentication transaction. A common ***credential*** is a User ID and associated password.

CSC See Section V-A.

Data Storage Media Any tape, CD/DVD disk, floppy diskette, cartridge, cassette, USB drive, flash drive, etc., that can potentially be used to store electronic files.

DPL See Section V-B.

Encryption A technique to protect the ***confidentiality*** of ***information.*** The method transforms ("encrypts") readable ***information*** into unintelligible text through an algorithm and associated cryptographic key(s).

Information Any information created, stored in temporary or permanent form, filed, produced or reproduced by, regardless of the form or media. Information shall include, but not be limited to:

- Personally identifying information
- Reports, files, folders, memoranda
- Statements, examinations, transcripts
- Images
- Communications

If information is already legally in the public domain (e.g., under FOIL), it can be considered as 'public' information. As such security controls are not required to maintain its confidentiality.

Information Owner An individual or organizational unit responsible for making classification and control decisions regarding use of information.

Integrity "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

- Authenticity: A third party must be able to verify that the content of a message has not been changed in transit.
- Non-repudiation: The origin or the receipt of a specific message must be verifiable by a third party.
- Accountability: A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

ISO See Section V -D.

ITA See Section V -C.

Physical A generic description of any area containing non end-user IT equipment and subsidiary ***infrastructure*** hardware, e.g.,:

- Mainframes
- Servers
- Communications equipment
- Printing facilities
- Media libraries
- Wiring closets

Portable Computers Equipment used for the processing of information that connects or can connect wirelessly to its data source and can be easily moved without extra assistance. This includes, but is not limited to, tablet, smart phones, blackberries, laptops, and netbook.

Privacy The right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.

Risk A ***risk*** is defined as where there are inadequate controls to mitigate a ***threat*** or ***vulnerability*** effectively. There are two elements to determine the import of a ***risk***:

- Impact- health and safety, reputational, legal and regulatory, financial, etc.
- Likelihood- likely to occur daily, weekly, etc.

Supervisor An individual responsible for day-to-day management or supervision of a ***User***.

System An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications.

Third Parties Anyone directly or indirectly providing goods and services to DOCCS who is not under the direct control of DOCCS.

Threat The potential for a person, object, or event to negatively impact the security of the ***physical infrastructure, systems,*** or ***information***. Threats can be malicious, such as the intentional modification of sensitive information, or they can be accidental, such as an error in a calculation, or the accidental deletion of a file. Threats can also be acts of nature, e.g., flooding, wind, or lightning, etc.

Other threats include:

- Hacking
- Inability to access the datacenter
- Denial of service
- Loss of key staff
- Virus
- Data corruption
- Destruction of assets

User Any person authorized by the information owner to access the system for a legitimate governmental purpose

Vulnerabilities Weaknesses in a system, application, or operating environment that can be exploited by a ***threat***. For example, unauthorized access (the ***threat***) to a system or application could occur by an outsider guessing an obvious password.

The vulnerability exploited is an easily guessable password chosen by a user. Reducing or eliminating the vulnerabilities can reduce or eliminate the ***risk*** to the system, application, or data. For example, a tool that can help users choose robust passwords may reduce the chance that they will choose readily guessable passwords and thus reduce the ***threat*** of unauthorized access.

Wireless Data Networking Equipment
Any device that enables a user to transmit data wirelessly (excluding cell phones and pagers governed by DOCCS Directive #2917, "Cellular Telephones and Pagers"). Examples include, but are not limited to, any device capable of the following: Bluetooth, WiFi, InfraRed, etc.

Workforce State employees and other persons whose conduct, in the performance of work for DOCCS, is under the direct control of DOCCS, whether or not they are paid by the Agency.

STATE OF NEW YORK

DEPARTMENT OF CORRECTIONS AND COMMUNITY SUPERVISION

THE HARRIMAN STATE CAMPUS – BUILDING 2

1220 WASHINGTON AVENUE

ALBANY, N.Y. 12226-2050

BRIAN FISCHER
COMMISSIONER

JOSEPH F. BELLNIER
DEPUTY COMMISSIONER
CORRECTIONAL FACILITIES

TO: All Superintendents

FROM: Joseph F. Bellnier, Deputy Commissioner

SUBJECT: Laptop/Mobile Computers in Facilities

DATE: December 8, 2011

This memorandum will provide direction regarding the introduction of laptop computers, mobile computers and related devices into a correctional facility. It compiles, revises, and expands upon previous memoranda on the subject.

The following are conditions where laptop/mobile computers are authorized for introduction into the facility:

Facility OSC Audit: As per Directive #2799, during facility audits by the Office of the State Comptroller, the audit liaison from the Bureau of Internal Controls (BIC) will arrange with the superintendent or designee for the auditors to enter the facility with a laptop computer. Auditors may **not** hook up their modems to phone lines while inside the facility or utilize laptop computers with wireless capability. Laptop computers will not remain in the facility overnight.

Basic Statewide Requirements: All laptops and removable media that have been authorized for use within the facility (disks, flash drives, etc.) are required to have full-disk encryption in accordance with New York State Office of Cyber Security, Policy P03-002, which is available at www.cscic.state.ny.us. In addition, all laptops must be configured to require Boot Authentication – requiring at a minimum, a User-ID and Password upon the power-up of the device. All removable media is to be treated as a Class-A tool and treated accordingly.

Construction: Individuals responsible for construction/physical plant projects that require a laptop computer and/or camera(s), including digital cameras, to evaluate, review, program, reprogram, adjust or otherwise maintain facility equipment, may bring the above-referenced equipment into the facility under the following conditions:

1. The laptop computer and/or camera(s) must be placed on a gate clearance and specific approval given by the superintendent.

2. The laptop computer and/or camera(s) must not remain in the facility overnight. The equipment must enter and exit the facility with the contractor.

3. The laptop computer and/or camera(s) must be under the supervision of facility staff assigned when connected to any telephone line. Only those photographs that are necessary to evaluate the project will be allowed.

4. The laptop computer may not be equipped with any wireless communication device (i.e., cellular, wireless broadband or other wireless modem) enabling wireless access to the internet, remote computers or persons. Additionally, the computer may not include a camera or contain a rewritable CD/DVD device. (**NOTE**: This does not include internal components such as Wireless Lan, Wireless Fidelity ("Wi-Fi") or blue tooth capabilities -- all of which should be disabled prior to entering the facility.)

Court Stenographers: Court stenographers, including court stenographers for parole hearings, are approved to bring laptop computers into the facility under the following conditions:

1. The laptop computer must be placed on a gate clearance and specific approval given by the superintendent.
2. The laptop computer must not remain in the facility overnight. It must enter and exit the facility with the stenographer.
3. The laptop computer may not be connected to any telephone line or Department network connection.
4. The laptop computer may not be equipped with any wireless communication device (i.e., cellular, wireless broadband, or other wireless modem) enabling wireless access to the Internet, remote computers, or persons. (**NOTE**: This does not include internal components such as Wireless LAN, Wireless Fidelity (Wi-Fi), or Bluetooth capabilities – all of which should be disabled prior to entering the facility.)
5. The stenographer must complete and sign the attached "Acknowledgment of Conditions for Entry of Computer into Correctional Facility" form. The acknowledgment form should be maintained with the gate order.

Parole Commissioners: Each Parole Commissioner entering a correctional facility for the purpose of conducting parole hearings will be permitted to bring a Division of Parole provided laptop computer and a portable USB-connected printer with them. The following conditions shall apply:

1. The laptop computer and printer may be carried in a briefcase or separate carrier and must be declared to processing staff and its presence noted in the facility entry log. It will not be necessary to inspect the device in any way.
2. The laptop computer may not be equipped with any wireless communication device (i.e., cellular, wireless broadband or other wireless modem) enabling wireless access to the Internet, remote computers or persons. Additionally, the computer may not include a camera or contain a rewritable CD/DVD device. (**NOTE**: This does not include internal components such as Wireless LAN, Wireless Fidelity ("Wi-Fi") or blue tooth capabilities – all of which should be disabled prior to entering the facility.)
3. The laptop computer may not be connected to any telephone line or Department network connection.
4. It must enter and exit with the Parole Commissioner.

Outside Vendors: Many outside vendors are equipped with mobile computers that are utilized to track and inventory shipments to customer sites. These devices are hand-held, may contain a global positioning system (GPS), may facilitate wireless communications from inside the facility and are usually carried and operated by the delivery person. The following procedure will apply to outside vendors making deliveries into our facilities utilizing these types of electronic devices:

1. Vendors will declare and surrender the mobile computer to staff prior to entering the facility and have it returned upon exit.
2. If the use of a mobile computer by a vendor is necessary or required to perform a task within the facility, a request will be submitted and processed in accordance with the guidelines for "**other laptop/mobile computer requests.**"

Other Laptop/Mobile Computer requests: All other requests to bring any laptop computer into a correctional facility must be specifically approved by the Commissioner. The request is to be addressed via e-mail to the Director of MIS, who will forward it with a recommendation to the Commissioner.

Blackberries: Blackberries are **not** allowed inside a correctional facility without the specific approval of the Commissioner.

If you have any questions regarding the authorization process or use of the above-referenced equipment, contact your Assistant Commissioner for Correctional Facilities.

Attachment