NEW YORK STATE Department of Corrections and Community Supervision **DIRECTIVE**	TITLE **Information Security Policy**		NO. 2810 DATE 06/30/2022
SUPERSEDES DIR# 2810 Dtd. 09/02/14	DISTRIBUTION A	PAGES PAGE 1 OF 17	DATE LAST REVISED
REFERENCES (Include but are not limited to) See Section II	APPROVING AUTHORITY Anne Marie McGrath		

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 technology infrastructure and to define specific controls necessary to support that purpose within the Department's unique operating environment.

II. REFERENCES

- 44 U.S.C., Sec. 3542
- NYS ITS Policies
  - NYS-P08-002
  - NYS-P14-001
- Executive Order Numbers 1, 2, 7, and 117
- ACA Expected Practices
  - 5-ACI-1F-02, 5-ACI-1F-03, 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-06, 5-ACI-1F-07
  - 2-CO-1F-06
  - 2-CI-2C-1, 2-CI-2C-2
- Directives #2011, #2799, #2821, #2822, #2824, #2917, #2944, #2948, #6920

III. POLICY: The Department of Corrections and Community Supervision (DOCCS) technology resources must be restricted from unauthorized access and used in a manner that is consistent with DOCCS security policies and procedures citied herein. DOCCS technology resources may be used solely in the conduct of official Departmental business except for incidental personal use that does not conflict with the proper exercise of the duties of the State employee.

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, the authority to oversee, direct, and coordinate the establishment of information technology policies, protocols, and standards for State Government. Further details of this authority can be found in NYS ITS Policy NYS-P08-002. Consistent with this authority, DOCCS shall follow all policy as promulgated by the *New York State Chief Information Officer (CIO)/New York State Office of Information Technology Services (ITS)* and the *New York State Office of Cyber Security (OCS)*, which can be found at https://its.ny.gov/. For the purpose of this directive, staff should be familiar with NYS ITS Policy NYS-P14-001 "Acceptable Use of Information Technology Resources" and DOCCS Directive #2824, "Use of Electronic Mail (Email)."

Pursuant to former Governor Cuomo's Executive Order No. 2, "Review, Continuation and Expiration of Prior Executive Orders," authorizes the continuation of 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 "https://governor.ny.gov/," through the Executive Orders link.

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.

IV. APPLICABILITY: The provisions of this directive are applicable to all DOCCS technology resources and all personnel or incarcerated individuals using those resources.

V. 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, as detailed in Directive #2822, "Request for Information Technology Hardware Acquisition/Relocation/Removal."
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. All DOCCS physical locations must have a designated Computer Security Coordinator (CSC) and Data Processing Liaison (DPL).
4. The DPL or designee at each physical location will ensure that proper inventory records of all 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 as requested. All inventory policies are governed by and detailed in Directive #2944, "Equipment Control," and Directive #2948, "Reporting Loss of Issued Items."
5. Facility computer equipment shall be relocated in accordance with Directive #2822, "Request for Information Technology Hardware/Acquisition/Relocation/Removal."
6. All Information Technology (IT) equipment must be approved by the Office of Strategic Planning and Population Management and ITS prior to purchase and installation.
7. 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.

8. Only properly licensed software that has been authorized by ITS may be installed. ITS will perform all installations.
9. Security testing software, including sniffers, scanners, and vulnerability assessment tools may not be installed on Department owned computer equipment unless specifically authorized by the ITS Information Security Office (ITS ISO). ITS will perform all installations.
10. No programs or applications are to be developed and placed into production without the written approval of ITS as detailed by 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 technology 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 technology resources of the Department against unauthorized use, theft, sabotage, and natural or man-made disasters.
3. Computer monitors 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 ITS 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 are configured, administered, and maintained according to DOCCS/ITS standard configuration and DOCCS information security policies, as approved by the ITS ISO.
2. All computer terminals 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 ITS ISO.

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 ITS 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 incarcerated individuals 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.
3. ITS shall assign a unique User ID to DOCCS personnel and other authorized individuals requiring access to systems and applications.
4. Individuals requiring access in excess of what has been identified on the pre-approved access grid to a DOCCS application are required to submit an ITSM ticket to ITS identifying the correct Central Office Executive Team member who will review and render a determination. Only 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 90 days and cannot be one of the last 24 passwords used.
9. Passwords must be at least 14 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 submit an ITSM ticket to ITS 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 Chief Information Security Officer (CISO) in the event a user, administrator, or system password is compromised or reasonably believed to be compromised.

G. Document Security

1. Instruction manuals, operating instructions, diagrams, and other sensitive information must not be left unattended and must always be secured and controlled. Incarcerated individuals or parolees 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. 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. 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 are the responsibility of the employee. For further information regarding remote connection concerns, please reference: https://its.ny.gov/tables/technologypolicyindex.

I. Wireless Communication/Networking

1. The use of wireless voice communications is governed by Directive #2917, "Cellular Telephones and Pagers."
2. Wireless data networking equipment is prohibited in all DOCCS facilities and locations, including but not limited to wireless computer mice, keyboards, printers, scanners, fax machines, etc.
3. Wireless network equipment, with the exception of the below, are prohibited in all DOCCS facilities and locations.
4. Wireless devices required for the operation of the incarcerated individual phone system tablet program in restricted housing areas will be allowed with approval of the Deputy Commissioner for Strategic Planning and Population Management in consultation with the ITS ISO.

5. Wireless metering devices required for DOCCS to comply with Executive Order 88, regarding the collection of energy usage data are allowed with the following provisions:
    a. Metering devices will be connected to existing or newly installed facility network wiring wherever feasible, unless cost prohibitive.
    b. Vendors providing wireless metering devices will sign a Service Level Agreement (SLA) guaranteeing wireless signals from such metering devices meet required security protocols.
    c. The ITS ISO will review the deployment of the devices in each facility prior to installation.
    d. All installations will be reviewed semi-annually to ensure the wireless transmission remains secure.

NOTE: The use of wireless-enabled laptops is prohibited as documented by subsection VIII-H-3(e)(4).

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 Directive #6920, “System of Internal Controls.”

VI. ROLES AND RESPONSIBILITIES

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

1. Inform facility/area office/unit personnel of DOCCS computer security policies and standards.
2. Serve as the facility/area office level point of contact regarding computer-related security matters.
3. Establish controls and procedures for implementing computer security measures.
4. Resolve issues with regard to shared computer resources among different organizational units.
5. Conduct periodic reviews to monitor and evaluate the facility’s computer security.
6. Assist the Information Security Office with facility level audits and inspections as requested by the ISO.
7. Implement all computer security provisions and initiate corrective actions.
8. Report any breach of computer security to the Superintendent, Central Office Division Head, or Regional Director and the CISO.
9. Maintain accurate records of personnel authorizations.
10. Conduct audits in coordination with the Office of Strategic Planning and Population Management, at a minimum annually, based on the 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. Submit ITSM requests with a list of changes and deletions based on the audit findings.

d. Retain these documents as a permanent record of the audit review.

11. Review the equipment, its configuration, and the practices in place regarding the use of equipment provided for an incarcerated individual training program to verify compliance with this directive.

12. Obtain from the staff advisor of an incarcerated individual 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 the initial problem determination for computer hardware with the guidance and support of ITS and equipment vendors.

2. Coordinate requests sent to ITS for terminals, printers, and thin clients using the procedures outlined in Directive #2822, "Request for Information Technology Hardware Acquisition/Relocation/Removal."

3. Assist in equipment placement decisions.

4. Field all help and service calls within the facility/area office and determine appropriate action.

5. 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.

6. Facility staff responsible for computer equipment used for incarcerated individual training shall maintain and provide to the DPL an inventory of all equipment and a description of any networking of that equipment.

7. Assist in training facility personnel in the proper use of Department computer equipment.

8. Inform the Public Safety Contact Center when a generator test is scheduled.

9. Read e-mail and SYSM bulletin board regularly.

VII. 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 **Cyber Command Center** at **518-242-5045.**

The Cyber Command 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*.

In accordance with a February 14, 2018, memorandum from the Director of State Operations, for any cyber incidents defined as Potential High Level Cyber Incidents, the Deputy Commissioner for Strategic Planning and Population Management will be notified immediately and in turn will make notification directly to the NYS Chief Information Security Officer (CISO), the Deputy Secretary for Public Safety, and the Assistant Counsel for Public Safety within the Executive Chamber.

Potential High Level Cyber incidents for the purpose of this notification, are when any of the following circumstances are present:

- There is a cyber incident or threat that significantly impacts, or has the potential to significantly impact public health, safety, or economic security.
- There is a cyber incident or breach that results in the compromise of a substantial quantity of personally identifiable information or other sensitive information.
- An incident significantly impacts other federal, state, or local government agencies in the United States; or
- A cyber incident receives significant media attention.

VIII. 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/intranet accessibility and service contributes broadly to the mission of the Department.

The internet/intranet connection and services, including electronic mail, 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/intranet facilities by any employee or other person must be requested and approved in accordance with ITS Policy. 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. To circulate unauthorized solicitations or advertisements for non-state purposes including religious, political, or not-for-profit entities,
3. For commercial or purposes in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, business transactions),
4. Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable unwanted email content using State information technology resources,
5. For activities unrelated to official assignments and/or job responsibilities,
6. For any illegal purpose,
7. To knowingly transmit/receive threatening, profane, or harassing materials or correspondence,
8. For unauthorized distribution of NYS data and information,
9. To interfere with or disrupt network users, services, or equipment,
10. 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,
11. To download, upload, or exchange music or video files without specific authorization by the ISO,
12. To download, upload, or exchange commercial, freeware, or shareware software that has not been approved by the ISO,
13. For electronic messaging including instant messaging (IM) and internet e-mail that has not been explicitly approved by the ISO,
14. To download, upload, or transmit sexually explicit, violent, or otherwise offensive material,
15. 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,
16. For any Union activity other than in preparation for labor/management meetings. "Preparation" shall exclusively mean informing Union members of the time and location of said labor/management meetings, as well as informing Union members of the topics on the agenda of said meetings,

17. For private advertising of products or services, or
18. For any activity meant to foster personal gain.

D. Occasional and Incidental Personal Use: Occasional or incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy and the requirements of Executive Order No. 7[1], is limited in amount and duration, and does not impede the ability of the individual or other uses to fulfill the State Entity's responsibilities and duties, including but not limited to, extensive bandwidth, resource or storage utilization. State Entity may revoke or limit this privilege at any time.

For example, users may make occasional and incidental personal use of information technology resources to schedule a lunch date, cancel a sports practice, check their bank accounts or other personal investment, or to communicate with a volunteer charity organization.

Your judgement regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgement by providing the above guidelines. If you are unclear about the acceptable "personal" use of a State-provided resource, seek authorization from your immediate supervisor.

E. Guidelines for Personal Use of Social Media: Staff shall be sensitive to the fact that information posted on social media sites clearly reflect upon the individual and may also reflect upon the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to restrict, as it often lives on in copies, archives, back-ups, and memory caches.

F. Agency Rights: DOCCS personnel should have no expectation of privacy relative to the use of DOCCS systems and applications, including electronic messaging and internet usage. Authorized personnel, including staff of the Information Security Office, have access to communications and may monitor messages as necessary to assure efficient performance and appropriate use, subject to the approval of the ITS Information Security Office. ITS maintains logs of all internet sites accessed. 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.

---

[1] Executive Order No. 7 **Prohibitions Against Personal Use of State Property and Campaign Contributions to the Governor** states, among other things, that: State computers shall be used only for official business, except that state computers may be used for incidental and necessary personal purposes.

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:

- Any costs, liabilities, or damages caused by the way the user chooses to use their 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.

G. 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 Office of Strategic Planning and Population Management. Other questions about appropriate use should be directed to the employee's 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.

H. Additional Restrictions Inside DOCCS Correctional Facilities (Staff)

1. Laptops and other computer equipment are prohibited from entering a correctional facility unless specifically authorized by the Deputy Commissioner for Strategic Planning and Population Management, or as detailed in subsection VIII-H-3.
2. The following guidelines are applicable to all Department issued or officially approved computer equipment as designated in subsection VIII-G-1:
   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.
3. There are circumstances where outside State Agency staff, Court Stenographers, visiting Departmental staff, outside vendor staff, or contracted service personnel will be required to bring a laptop or personally-owned computer to a correctional facility. The following instances are preapproved; however, the equipment must be placed on a gate clearance and the individual must complete the "Acknowledgement of Conditions for Entry of Computer in Correctional Facility Form." The completed form shall be maintained with the gate order.

a. **Audits conducted by the Office of the State Comptroller (OSC)**: As per Directive #2799, "External Audit Protocol and Response Procedures," during facility audits by OSC, 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** connect their technology devices to any network. Laptop computers will not remain in the facility overnight.

b. **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 conditions outlined at the end of this section.

c. **Court Stenographers**: Court stenographers, including court stenographers for parole board hearings, are approved to bring laptop computers into the facility under conditions outlined at the end of this section.

d. **Parole Board Members**: Each Parole Board Member entering a correctional facility for the purpose of conducting parole board hearings will be permitted to bring a DOCCS provided laptop computer and a portable USB-connected printer with them. The conditions outlined at the end of this section shall apply.

e. The following conditions apply in the above-outlined circumstances:

(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 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.

(3) The laptop computer and/or camera(s) must not remain in the facility overnight. The equipment must enter and exit the facility with the entity that brought the device with them.

(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 rewriteable CD/DVD device.

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 laptop computer may not be connected to any telephone line or Department network connection except as necessary by a contractor in their official capacity, when this becomes necessary, it must be under the supervision of facility staff.

(6) Only those photographs that are necessary to evaluate the project will be allowed.

f. **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 referenced in subsection VIII-H-3.

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 Directive #2822. The DPL will register, inventory, and configure the device according to DOCCS standards.

I. Additional Restrictions on Incarcerated Individuals

1. Incarcerated Individual 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 incarcerated individuals may access computer systems pending Superintendent approval:

a. Authorized use of the Incarcerated Individual Network (Law Library, etc).
b. Authorized training and/or educational activities.
c. Authorized 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 incarcerated individual 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 individuals."

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 incarcerated individual have in their personal possession any computer storage media outside of their 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 incarcerated individual 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 incarcerated individual 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.
5. Color printers or multi-functional devices with scanning or faxing capabilities are prohibited for this purpose, only black and white printers will be authorized.

IX. 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 subsection VI-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 subsection VI-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 Technology Resources Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, internet, email, and social media sites

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.

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 Technology 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 tablets, smart phones, laptops, and netbooks.

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 governed by Directive #2917). Examples include, but are not limited to, any device capable of the following: Bluetooth, Wi-Fi, 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.

Statewide technology policies, standards and guidelines may be found at the following website: https://its.ny.gov/tables/technologypolicyindex/.