

 State of Connecticut Department of Correction ADMINISTRATIVE DIRECTIVE	Directive Number 4.6	Effective Date 10/22/15	Page 1 of 8
	Supersedes Use of Computers and Related Technologies, Dated 1/9/2015		
Approved By:  Commissioner Scott Semple	Title Use of Computers and Related Technologies		

1. **Policy.** Computers and related technologies shall be utilized for authorized Department of Correction business only and consistent with state and federal law. The Department shall implement and monitor preventive measures to guard against the loss of state data. Each employee authorized to access information systems shall be trained by their Supervisor or designee prior to use of any information system relevant to their position.

2. **Authority and Reference.**
 - A. Connecticut General Statutes, Sections 1-18, 1-200, 1-218, 1-240, 4d-2(c)(1), 7-109, 18-81, 31-48d and 53-153.
 - B. Office of the Public Records Administrator and State Archives, General Letter 2009-2 June 30, 2009
 - C. Electronic and Voice Mail Management and Retention Guide for State and Municipal Government Agencies.
 - D. State of Connecticut Office of Policy and Management, Policy IT-REC-15-01, Electronic Mail Records Management Policy, June 15, 2015
 - E. State of Connecticut Comptroller's Office, Property Control Manual, September 2001.
 - F. Connecticut Software Management Policy by the State of Connecticut Office of the State Comptroller, the Office of Policy and Management and the Department of Administrative Services.
 - G. State of Connecticut, Department of Administrative Services/Bureau of Enterprise Systems and Technology (DAS/BEST), Acceptable Use of State Systems Policy, May 2006.
 - H. State of Connecticut, Department of Administrative Services/Bureau of Enterprise Systems and Technology (DAS/BEST), Policy on Security for Mobile Computing and Storage Devices, September 2007.
 - I. Administrative Directives 4.4, Access to Inmate Information; 4.7, Records Retention; 6.6, Reporting of Incidents; and 10.7, Inmate Communications.

3. **Definitions/ Acronyms.** For the purposes stated herein, the following definitions apply:
 - A. **Confidential or Restricted State Data.** Confidential or restricted state data includes, but is not limited to, the following:
 1. Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual.
 2. Organizational information that is not in the public domain and if improperly disclosed might:
 - a. cause a significant or severe degradation in mission capability;
 - b. result in significant or major damage to organizational assets;

Directive Number 4.6	Effective Date 10/22/15	Page 2 of 8
Title Use of Computers and Related Technologies		

- c. result in significant or major financial loss; or,
 - d. result in significant, severe or catastrophic harm to individuals.
 - B. DAS/BEST. Department of Administrative Services/ Bureau of Enterprise Systems and Technology.
 - C. Electronic Mail (e-mail). The electronic transfer of information typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties via an intermediate telecommunications system. E-mail is the means of sending messages between computers using a computer network. E-mail services, as defined by this policy, refer to the use of state-provided electronic mail systems.
 - D. Internet. A network of networks in which users at any one computer can retrieve information from another computer. The worldwide web is the most widely used part of the Internet.
 - E. MIS. Management Information Systems.
 - F. Mobile Computing Device. A portable computing and telecommunications instrument that includes, but is not limited to, notebooks, palmtops, PDAs, iPods®, BlackBerry® devices, and cell phones with Internet browsing capability.
 - G. Mobile Storage Device. A portable memory storage instrument that includes, but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.
 - H. Non-Record. Extra copies kept for convenience, informational copies of correspondence, duplicate copies of documents maintained in the same file, working papers and preliminary drafts.
 - I. Password. A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource.
 - J. Public Records. Department generated books, files, papers, audio/video/digital recordings, and/or other documents, in either paper or electronic format, which have been recognized by the State Librarian as having administrative, fiscal, or legal value.
 - K. Record. Any recorded data or information relating to the conduct of the public's business prepared, owned, used, received, or retained by a public agency, or to which a public agency is entitled to receive a copy by law or contract under Section 1-218 of the Connecticut General Statutes, whether such data or information be handwritten, typed, tape-recorded, printed, Photostatted, photographed, or recorded by any other method.
 - L. Secure Mobile Device. A mobile device that has a sufficient level, as defined by this policy and DAS/BEST standards, of access control, protection from malware and strong encryption capabilities to ensure the protection and privacy of state data that may be stored on the mobile device.
 - M. Software Package. Any program or application that can be installed on a computer.
 - N. Username. A name used to gain access to a computer system.
4. Employee Usernames and Passwords. Individual users are issued their own Username and initial password. Their username and password are for their use only and shall not be shared with anyone.

Employees are responsible for anything done on a computer system under their username.

Directive Number 4.6	Effective Date 10/22/15	Page 3 of 8
Title Use of Computers and Related Technologies		

Employees shall not use the browser capacity to remember passwords. Employees shall enter the password each time they log on. Each employee is responsible to take reasonable means to keep their password physically secure. Employees shall log off before leaving their work area or make sure that their computer is in "locked" mode before leaving their work area. Employees shall not leave any open and signed on computer unattended.

5. Use of Computers and Software. All federal and state law regarding the use of computers, networks and personal conduct shall apply to the use of Department computers and related technologies. The use of computers shall be for Department business only. Personal use of Department computers and related technologies shall be strictly prohibited. On a yearly basis, the Director of MIS will issue a memo to the Department employees reminding the staff of the policy that computers must be used for business purposes only and not for unauthorized use. Department employees shall comply with the following principles regarding the use of computers:
 - A. Any computer or software utilized by Department staff shall be authorized by the Department's Management of Information Systems (MIS) Unit, the Superintendent of Unified School District #1 (USD#1), or the Director of Correctional Enterprises of Connecticut (CEC). The use of personally owned hardware or the installation of shareware, freeware, personal or demonstration software, to include non-approved screen savers and computer games, shall be prohibited. The Director of MIS may issue a memorandum allowing specific departmental units to install shareware, freeware or demonstration software when the unit would benefit from the use of such software.
 - B. A software package shall be used on one computer at a time, unless the individual software license specifies otherwise.
 - C. A software package may be copied to diskette or compact disc (CD) for the purpose of making a back-up disc(s) to protect from loss.
 - D. Department computers and equipment, to include CD burners, shall not be used for copying personal information or software. The Unit Administrator or designee shall maintain a list of all computers equipped with a CD burner and their location.
 - E. Software purchased for network use shall be subject to the maximum number of simultaneous users specified by the software license. Under no circumstances shall a Department employee download an application from the Department's network server to an individual hard-drive without the written approval from the MIS Unit or in the case of education staff, the Superintendent of Unified School District #1.
 - F. The MIS Unit, USD#1 and CEC shall maintain a list of software that may be used on their respective computer systems. Requests to purchase any software package(s) for USD#1 use only must be forwarded to the Superintendent of USD#1 or designee for approval. Requests to purchase any software package(s) for CEC use only must be forwarded to the Director of Correctional Enterprises or designee for approval. Requests to purchase any software package(s) that is to be installed on any LAN access state computer must be approved by the Director of MIS.

Directive Number 4.6	Effective Date 10/22/15	Page 4 of 8
Title Use of Computers and Related Technologies		

- G. Software licensed to the Department of Correction shall not be loaned or given to any person or organization.
- H. The use of utilities that modify computer hardware configurations shall be prohibited.
- I. Inmates shall be prohibited from using computers except when necessary for specific educational or work assignment. Inmates shall not use any computer that is connected to a network of any kind, with the exception of the following:
 - 1. Education or CEC computers that are linked by a closed network hub, which shall not provide Internet access.
 - 2. Programmatic computers that are linked to a network for use by inmates through authorized facility sites allowing access to websites authorized by the Director of MIS or his/her designee. These sites may include the Department of Labor website, CT Distance Learning, Community Colleges, etc. Sex offenders are prohibited under Connecticut general Statute §18-81u from using a computer with internet access.
 - 3. Programmatic computers that are linked to a network for use by inmates on community supervision in order to perform programmatic functions. Such permission shall be in writing and shall cite the limits of authorization as a condition of supervision. Sex offenders are prohibited under Connecticut general Statute §18-81u from using a computer with internet access.
 - 4. Under direct supervision of a USD #1 staff member, inmates receiving legally mandated virtual services or attending pre-approved educational meetings may view the display of a staff members' computer solely for the purpose of attending the service/meeting. Under no circumstance shall an inmate operate, access, or otherwise have physical control of the staff member's computer, including the keyboard, mouse, touchpad, or any other input device.

All inmate access to computers shall be closely monitored and no inmate shall be allowed personal use of a computer for any reason.

- J. Each facility shall establish and implement procedures to ensure the security and accountability of computer discs where inmates may have access to them (e.g., maintenance shop, school, etc.). A logbook shall be used to maintain an inventory of all blank and programmed discs. Each disc shall receive a unique number which shall be recorded in the logbook. Inmates may be permitted to use computer discs for appropriate work related assignments and educational programs. Requests for educational discs, to include religious and non-religious correspondence courses, shall be made through the institutional religious facilitator, school principal or educational administrator, as appropriate. All correspondence courses that contain computer discs shall be reviewed in accordance with Administrative Directive 10.7, Inmate Communications prior to being released for use by the inmate. In no case shall inmates be allowed to move discs from their assigned work/education area to another area without authorization. Possession of discs in the inmate's living area or use of discs for personal purposes without proper authorization

Directive Number 4.6	Effective Date 10/22/15	Page 5 of 8
Title Use of Computers and Related Technologies		

from the appropriate supervisor shall be strictly prohibited and shall subject the inmate to disciplinary action.

- K. The facility shall perform periodic audits to ensure that all software standards are maintained. Audit results shall be forwarded to the Unit Administrator for review and follow-up action, as required.

6. Security for Mobile Computing and Storage Devices. Each DOC employee shall implement the appropriate level of security to guard against the loss of confidential or restricted state data as follows:

- A. No confidential or restricted state data shall reside on any mobile devices except as set forth in Section 5(B) of this Directive. The Department shall utilize secure remote data access methods, as approved by DAS/BEST, in support of mobile users.
- B. In the event utilization of secure remote access methods are not possible, the Department shall adhere to the following restrictions and requirements:
 - 1. The Commissioner or designee must authorize and certify in writing, in advance, that the storing of restricted and confidential state data on the mobile device is necessary to conduct state business;
 - 2. The Commissioner or designee must determine and certify in writing that reasonable alternative means to provide the user with secure access to that state data do not exist;
 - 3. The Commissioner or designee must assess the sensitivity of the data to reside on a secure mobile device and determine that the business need necessitating storage on the mobile device outweigh(s) the associated risk(s) of loss or compromise; and,
 - 4. The Commissioner or designee must authorize, in writing, the storage of specific state data on a secure mobile device and the acceptance of all associated risk(s).
- C. State data that the Commissioner or designee has authorized to be stored on a secure mobile device shall be:
 - 1. the minimum data necessary to perform the business function necessitating storage on the mobile device;
 - 2. stored only for the time needed to perform the business function;
 - 3. encrypted using methods authorized by DAS/BEST;
 - 4. protected from any and all forms of unauthorized access and disclosure; and
 - 5. stored only on secure mobile devices in accordance with Section 2(G) of this Directive.
- D. Any state data placed on a mobile device shall be documented, tracked, and audited by the Warden, Director, Supervisor or their designee for the unit or employee requesting to use a mobile device. Once the information has been documented on a Mobile Data Control Form, a copy of the form should be sent to the Director of MIS or his/her designee for their review. The information tracked shall include the identification of the individual authorizing storage of the data on the mobile device, the authorized user of the mobile device, the asset tag number of the

Directive Number 4.6	Effective Date 10/22/15	Page 6 of 8
Title Use of Computers and Related Technologies		

- mobile device (If applicable), information about the stored data, and the final disposition of the data .The MIS Unit shall configure mobile devices to allow only the minimum features, functions, and services needed to carry out state business.
- E. The MIS Unit ensure that mobile computing devices are configured with approved and properly updated software-based security mechanisms including anti-virus, anti-spyware, firewalls, and intrusion detection. Users shall not bypass or disable these security mechanisms under any circumstances.
 - F. Users in the possession of state owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas must not leave these devices unattended at any time, and must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft.
 - G. The Department shall establish and document reporting, mitigation and remediation procedures for lost or stolen mobile devices containing state data and for state data that is compromised through accidental or non-authorized access or disclosure.
 - H. In the event that a mobile device containing state data is lost, stolen, or misplaced, and/or the user has determined unauthorized access has occurred, the user shall promptly notify his or her supervisor of the incident. The Department shall promptly notify the DAS/BEST Help Desk of the incident in order to initiate effective and timely response and remediation.
 - I. The Department shall develop and implement a formal, documented security awareness and training program sufficient to ensure compliance with this policy.
 - J. The Department shall obtain a signed, formal acknowledgement from users indicating that they have understood, and agreed to abide by the rules of this Directive.
 - K. The Department and users shall adhere to this security policy and associated procedures; failure to do so may result in progressive discipline.
7. Use of Electronic Mail. The use of e-mail shall be for departmental business purposes only. The following principles shall govern the use of electronic mail:
- A. E-mail shall not be used to report incidents in accordance with Administrative Directive 6.6, Reporting of Incidents.
 - B. Using e-mail to solicit support for personal, political, or religious causes shall be prohibited.
 - C. The routine monitoring of e-mail by the MIS Unit shall normally be prohibited; however, the Commissioner or designee may direct the MIS unit to monitor, access and/or review employee e-mail.
 - D. Pursuant to General Letter 2009-2 from the Office of the Public Records Administrator; backup systems or tapes are not acceptable for the retention of electronic messages. Backups should only be used to protect vital records in the event of a disaster or to retrieve a record due to loss of data.
 - E. E-mail shall not be used in a manner that is deliberately wasteful of computing resources or which unfairly monopolizes resources to the exclusion of others. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages, creating unnecessary output of printing, or creating unnecessary network traffic.

Directive Number 4.6	Effective Date 10/22/15	Page 7 of 8
Title Use of Computers and Related Technologies		

- F. Employees who are issued electronic E-mail accounts and associated mailboxes are responsible for organizing their mailboxes and ensuring that any individual E-mails, calendar invitations, tasks, attachments and other applicable electronic data that meet the definition of a record or the definition of a public record are appropriately managed in accordance with the retention schedules set forth in Section 10 of Administrative Directive 4.7, Records Retention.
- G. Retention of E-mails and electronic data is based on the content of the message, not the media type. Employees shall evaluate the content of each E-mail that is sent or received for action and subsequent retention. Some Emails may be defined as "non-record" in accordance with section 3 of this Directive and can be deleted immediately upon receipt. Emails that document agency functions and provide evidence of agency business must be retained according to the equivalent records retention schedule that can be referenced in the Retention Schedules Folder attached to Administrative Directive 4.7, Records Retention.
- 8. Use of the Internet. The use of any Internet service for business unrelated to the Department shall be prohibited. The Unit Administrator or designee shall ensure that each employee with Internet access reviews, understands and signs CN 4601, Internet Use Agreement. The original CN 4601, Internet Use Agreement shall be forwarded to the facility personnel officer, who shall place the completed form in the employee's central personnel file. The MIS unit shall monitor each individual Internet account to prevent excessive or improper use. The following principles shall be in effect with regard to Internet usage:
 - A. The use of the Internet for an employee shall be approved by the Unit Administrator or higher authority prior to that employee utilizing Department equipment for that purpose.
 - B. Use of the Internet to gain unauthorized access to any computer system, application or service shall be prohibited. The Department shall monitor and audit the Internet usage within the agency to determine which sites are being accessed.
 - C. Use of the Internet for private commercial purposes, to include business transactions between individuals and/or commercial organizations shall be prohibited.
 - D. All electronic mail communication via the Internet shall be governed by the procedures included in Section 5 of this Directive.
 - E. The downloading of any software products via the Internet shall be subject to state and federal copyright laws. Any software downloads shall require the prior written approval of the MIS Unit. The downloading of files unrelated to department business shall be prohibited.
 - F. Any file downloaded from the Internet shall be scanned for computer viruses.
 - G. Use of the Internet that interferes with or disrupts network users, services or computers shall be prohibited. Such disruptions may include, but not be limited to distribution of unsolicited advertising, broadcasting unsolicited mailings or other messages, or propagation of computer viruses.
 - H. Use of the Internet to engage in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others shall be prohibited. These acts may include, but not be limited to, broadcasting unsolicited

Directive Number 4.6	Effective Date 10/22/15	Page 8 of 8
Title Use of Computers and Related Technologies		

mailings or other messages, creating unnecessary output, or creating unnecessary network traffic.

9. Access to Criminal Justice Information Systems and Training. All access to criminal justice information systems shall be authorized by the appropriate Unit Administrator or Division Head. The Unit Administrator or Division Head may designate an individual responsible for monitoring employee certification. For training purposes, a list of employees requiring initial certification or re-certification shall be forwarded to the Director of Training and Staff Development or designee. The Director of Training and Staff Development or designee shall coordinate required background checks with the Security Division and schedule training with the appropriate agency provider, specific to the appropriate criminal justice information system.
10. Use of Criminal Justice Information Systems. Use of any criminal justice information systems such as the Connecticut Online Law Enforcement Communications Teleprocessing (COLLECT), National Crime Information Center (NCIC), Judicial Information System (JIS), Offender Based Tracking System (OBTS), Paperless Re-Arrest Warrant System (PRAWN), and Judicial Electronic Bridge (JEB) shall be governed by the policies and procedures of those respective systems and in accordance with Administrative Directive 4.4, Access to Inmate Information.

Each Department employee who has access to information received via the COLLECT, NCIC, JIS, OBTS, PRAWN and/or JEB automated systems shall be required to review and sign CN 4402, Agreement to Protect Confidentiality of Computerized Criminal Record Data prior to use. The Unit Administrator or designee shall ensure that each employee signs form CN 4403 after returning from training. The signed original shall be forwarded to the facility personnel officer, who shall place the completed form in the employee's central personnel file.
11. Use of Electronic Health Records. All Access to Electronic Health Records (EHR) shall be authorized by the appropriate Unit Administrator or Division Head. Authorized users may only access the medical records of patients they are actively caring for, for legitimate, clinical or collaborative purposes.
12. Forms and Attachments. The following form is applicable to this Administrative Directive and shall be utilized for the intended function:
 - A. CN 4601, Internet Use Agreement.
 - B. Mobile Data Control Form V02
13. Exceptions. Any exceptions to the procedures in this Administrative Directive shall require prior written approval from the Commissioner.