



CONNECTICUT DEPARTMENT OF TRANSPORTATION

POLICY STATEMENT

POLICY NO. F&A-28

December 20, 2010

SUBJECT: Connecticut Department of Transportation Policy on Computer Systems Acceptable Use, Internet Code of Conduct, and Computer Security

This Policy (Policy) is put forth to Department of Transportation (Department) employees, employees of other State agencies, contracted vendors that conduct business with the Department, and all other parties who may use or access computer equipment and communications networks owned, operated or administered by the Department (hereinafter referred to as "User(s)"). Such computer equipment and communications networks include, but are not limited to, computer servers; state-issued shared or stand-alone computers (the word "computers" includes desktop computers, laptop computers, minicomputers, microcomputers); local area networks (LANs) and wide area networks (WANs); Internet access; and USB devices and handheld PDA devices (e.g., Blackberry) that combine computing, telephone/fax, Internet, and/or networking features (hereinafter collectively or individually referred to as the "Systems"). This Policy may be revised from time to time. The State of Connecticut Acceptable Use of State Systems Policy (State Acceptable Use Policy) is incorporated into this policy in its entirety, and is posted at www.ct.gov/doit - IT Policies. **To be clear, since the State Acceptable Use Policy is incorporated into this Department Policy on Computer Systems Acceptable Use, Internet Code of Conduct and Computer Security Policy, all Users are responsible for reading and complying with both.**

In accordance with the State of Connecticut Acceptable Use of State Systems Policy, State Systems and all information contained therein are State property. Information created, sent, received, accessed, or stored using these Systems is the property of the State. All activities involving the use of State Systems are not personal or private. Therefore, Users should have no expectation of privacy in the use of these resources. Information stored, created, sent, or received via State Systems is potentially accessible under the Freedom of Information Act. Pursuant to Section 31-48d of the Connecticut General Statutes and the State of Connecticut's "Electronic Monitoring Notice," the State reserves the right to monitor, log, and/or analyze all activities without notice. This includes, but is not limited to, correspondence via e-mail, voice-mail, and facsimile, including, but not limited to, e-mails sent or received on personal e-mail accounts using State Systems.

To re-emphasize: In addition to this Policy, the State Acceptable Use Policy applies to all Users (www.ct.gov/doit - IT Policies), and failure to comply with the same may result in disciplinary action up to and including termination.

1. **User Identification and Password:** Each User who requires access to Department Systems, following approval from their unit supervisor or manager, shall be issued a User Identification (UserID) and User Password. Users are required to take reasonable steps to prevent others from learning his/her UserID and Password. User Passwords must not be given to anyone. If a Password is compromised, or there is reasonable suspicion of compromise, the Password should be changed by the User or the person responsible for the specific system. Each User is responsible for information or materials accessed or processed using his/her UserID and Password:

- a. Where security software allows User Passwords to be changed by the User, the Password shall be changed frequently (a minimum of every three months).
 - b. Where security software requires the involvement of the Systems Administrator and the Office of Information Systems (OIS) to change User Passwords, the Password shall be changed every three months.
 - c. Additions and deletions of UserIDs and Passwords from any System is the responsibility of the designated system administrator for that particular hardware system and/or software application. A form available on the Department's Intranet site is required for adding or deleting UserIDs and Passwords.
 - d. Unit managers and the Office of Human Resources must notify the Security Office and OIS Management or OIS Help Desk as soon as possible of the date when an employee will terminate. Users with access to Department Systems will have their access to services and Systems terminated at the conclusion of their employment or earlier, as determined by the unit manager and the Office of Human Resources.
 - e. When an employee is promoted or reassigned, unit managers must evaluate the User's security level and initiate a request to the OIS System Administrator for appropriate changes to the security level for the new position. This can be accomplished through an e-mail to the OIS Help Desk.
2. Software Programs and Information residing on Department Systems will not be disclosed or copied by Users without appropriate authorization from OIS. Information released subject to Policy Statement No. EX.O.-14 regarding "Freedom of Information" is exempt from this requirement.
- a. Users are not permitted to install software on Department Systems. All software installations must be performed by OIS Support Staff with proper notification from the requestor, provided proper approvals by the employee's manager and Director of OIS have been obtained and required licensing has been acquired.
 - b. Full compliance with license agreements for all software products is required. Appropriate licenses required to install software products on Department Systems or the Department's network must be obtained by OIS, with OIS approval required prior to installation.
 - c. The installation of illegal, unlicensed, or unauthorized copies of software programs is prohibited and will be removed immediately by the designated OIS Data Security Officer or at his/her direction. Installation of personally owned software on Department Systems is strictly prohibited.
3. Modems expose Department Systems to network security concerns and, therefore, are prohibited unless specifically authorized by the Director of OIS. Alternative access methods will be considered by the OIS Data Security Officer in cases where there is sufficient business need for network connectivity. All requests or questions regarding network connectivity should be directed to the OIS Help Desk.
4. Remote Connectivity to the Department's network is available based on business need via a Virtual Private Network (VPN) connection installed on State-issued computers. In special instances, VPN may be installed on employees' home computers; however, the responsibility for the installation and maintenance on personal home computers or laptops will be the responsibility of the individual employee. Work at home VPN requests must be approved first by the Bureau Chief or his/her designee and then submitted to Human Resources for final approval prior to being granted by OIS.

5. Laptops: All laptops must be encrypted with the encryption software approved by the Department of Information Technology. Laptop specifications must be approved by OIS prior to purchase to ensure compliance with State and Department technology standards. Laptops connected to the Department's wired and wireless network are primarily for training and presentation purposes. However, subject to a demonstrated business need and justification by a Bureau Chief, and with OIS Director approval, laptops can replace desktop computers using connections previously approved and with proper security and encryption software installed by OIS. Upon request by OIS staff, Users must make laptops available for technical review to verify correct technical configuration and adherence to security policies. Unauthorized configuration of a laptop will be referred to the User's supervisor or manager to determine the consequences of such usage. The use of laptops is subject to all provisions contained in this Policy applicable to computer use. If a laptop is lost, missing, or stolen, it must be reported immediately to the Department's Division of Security and OIS. When a laptop is to be used at an off-site location for an extended period of time, it is required that a Record of Equipment on Loan Form (CO-1079) be filed with the Division of Purchasing and Materials Management.
6. Wireless: Connections to the Department's wireless network will be limited by business need. State-issued laptops may be connected to the Department's wireless network in the Headquarters Building, Training Center, Data Center, and District Offices, where available, only for authorized purposes. Authorized vendors and suppliers may also connect to the wireless network if there is a business need, but only with prior approval and authorization by OIS.
7. Antivirus Software: State-issued computers have antivirus software installed to protect the Department's network infrastructure from computer viruses. Any identified or suspected virus contamination should be referred to the OIS Help Desk.
8. Internet: An Internet Code of Conduct establishes Internet usage guidelines for Users. The objective of this Policy is to avoid inappropriate Internet usage and potentially embarrassing situations. Although many inappropriate Internet web sites are blocked through Internet filtering, not every inappropriate site can be blocked due to the volatile nature of Internet information and search capabilities.

The Department of Information Technology and OIS have the technical capability to proactively monitor Internet usage and view web sites visited by Users. Usage reports can and will be made available for management review on an as needed basis. Additionally, if a supervisor suspects a User is violating the Internet Code of Conduct, he/she may submit a request through his/her manager for OIS to review or monitor the User's computer use.

The following Internet Code of Conduct Guidelines must be adhered to by all Department Internet Users:

- a. Access to the Internet through the Department's network will be used for Department business purposes only.
- b. Access to the Internet through non-State issued computers or by other non OIS approved technology means (i.e., modems) is prohibited.
- c. The Internet is to be used and web sites accessed for legitimate Department business purposes only. The Internet is not to be used for any other purpose including entertainment, leisure or personal activities. Examples of unacceptable Internet use include, but are not limited to, accessing web sites for shopping, booking trips, research, etc; downloading unauthorized software or inappropriate materials, Internet radio, chat room access, social networking sites (i.e., MySpace and Facebook), and instant messaging programs (i.e., AOL Instant Messenger, MSN Messenger, and similar programs).

- d. Users shall not access, view, or otherwise connect with non-Department work-related web sites; download, save, send, print, or e-mail the content therefrom, including, but not limited to, any inappropriate materials or subject matter, jokes, and any non-work related files. Access to such materials is tracked by the Department, and inappropriate materials may be recorded by the Department or otherwise retained on the computer. Spyware and adware software is not allowed on state-issued computers, as well as live weather data programs, search tools, and search toolbars. When Users detect these types of programs, they should notify the OIS Help Desk. When pop-ups occur, they should not be opened or accepted.
 - e. Users shall immediately report receipt of any unsolicited, inappropriate materials to his/her supervisor. The supervisor should then report it to OIS Management or OIS Help Desk.
 - f. Users must lock or log off their computers during any period of time they are away from their computers (i.e., meetings, breaks, lunch periods, end of the workday, etc.) to prevent unauthorized usage occurring when a User is logged on and away from his/her computer.
 - g. Users must not use the Internet in any unauthorized way that obligates the Department for payment of goods or services by entering into any agreements or contracts as a Department employee on behalf of the Department. All purchasing must be done through Core-CT.
 - h. Any personally owned or non-State issued computer equipment and software that may be operating independent of the Department's network, while the User is on State of Connecticut property or a Department worksite, shall not be used to obtain non-work related or inappropriate subject matter for display in the workplace or in other ways that violate the intent of this Policy.
9. Confidential Data: The storage of confidential or restricted data is prohibited on any mobile devices that include, but are not limited to, laptop computers, diskettes, magnetic tapes, external/removable drives, flash cards, thumb drives (USB keys), jump drives, compact disks, and digital video disks. This Policy is outlined in the Department of Information Technology Policy on Security for Mobile Computing and Storage Devices, Version 1.0, issued September 10, 2007. Individual Bureaus are responsible for determining data that is confidential or restricted.
10. USB Flash Drives must be purchased through the Department's purchasing approval process and are permitted for the portability and retrieval of non-confidential data only. The storage of confidential or restricted data on a Flash drive is strictly prohibited (refer to No. 10 above - Confidential Data). Personal or non-State issued flash drives are prohibited for use on Department Systems. Flash drives must not be bootable or used to launch applications. Users are responsible for the loss of removable drives and for safeguarding Department information at all times.
11. Personal Use: All Department Systems, including State-issued computers, are a government resource and are subject to the same rules as other government resources. Use of the Department's computers for personal use (i.e., anything non work-related) is strictly prohibited. Examples of prohibited personal use of Department Systems include, but are not limited to, accessing personal e-mail accounts (e.g., Gmail, Hotmail, Yahoo, etc) to send or receive personal e-mail; accessing web sites for shopping, booking trips, research, etc.; downloading unauthorized software or inappropriate materials; typing personal documents, Internet radio, chat room access, social networking sites (i.e., MySpace and Facebook), and instant messaging programs (i.e., AOL Instant Messenger, MSN Messenger, and similar programs). Personally-owned or non-State issued computer equipment and software are prohibited from State premises or from being used with the Department's data communications network.

12. **E-mail:** All e-mail messages are considered the property of the State and, as such, are considered public records. E-mails are not considered personal or private; therefore, Users should have no expectation of privacy or confidentiality with regard to the same. All e-mail messages are potentially accessible under the Freedom of Information Act. Any messages created, sent, received, accessed, or stored on Department Systems constitute Department records. The State and the Department reserve the right to monitor (pursuant to Section 31-48d of the Connecticut General Statutes) and/or log e-mail communications without further written notice. E-mail is stored on network backup tapes and is retrievable. The content and maintenance of a User's e-mail account is the User's responsibility. This responsibility includes checking e-mail daily and maintaining these public records as required under the State Agencies' Records Retention/Disposition Schedule S1: Administrative Records. Users can review the guidelines for managing and retaining electronic messages by referring to the Office of Public Records Administrator General Letter 2009-2. E-mails should be retained according to this General Letter to ensure they can be retrieved. Users should also refer to the Department's record retention schedules for proper procedures regarding disposition of e-mail communications and all correspondence must be maintained by subject as opposed to record type (e.g., if any of your e-mails are related to a construction project, these records must follow the retention period for that project). **Important Note:** If any of your e-mails are subject to a litigation hold, those e-mails must be retained notwithstanding the record retention schedule, until such time you are notified that the hold has been released.
13. **Illegal Activities:** Use of Department Systems for illegal purposes or activities is prohibited. Illegal activities include, but are not limited to, violations of local, State, and/or federal laws and regulations. Relevant Connecticut law includes, but is not limited to, Section 53a-251 et seq. of the Connecticut General Statutes. Section 53a-251 defines "computer crime." Included in the definition are: (a) unauthorized access to a computer system, (b) theft of computer services, (c) interruption of computer services, (d) misuse of computer system information, and (e) destruction of computer equipment.
14. **Administrative Rights** to any Department Systems are approved for OIS personnel ONLY.
15. **Games:** Playing or downloading computer games on Department Systems is strictly prohibited.

Internal Protocol for Alleged Computer Violations

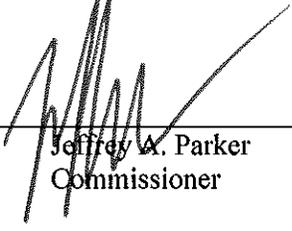
When there is an alleged computer usage violation, the following protocol will be followed:

1. Alleged violations should be reported to the Office of Human Resources.
2. Human Resources, OIS and Security will evaluate the allegation and develop an action plan for investigation.
3. If circumstances warrant, the Division of Security will seize the computer for analysis to determine if computer usage policies were violated. The Division of Security will work with OIS management to determine which internal and/or external sources will perform the analysis. **Note:** All allegations of pornography will be investigated by external sources and substantiation of pornographic materials found on state equipment will result in termination.
4. If circumstances warrant, the User's record of computer use will be reviewed, including, but not limited to, a review of e-mails sent and received and internet usage. OIS management will determine who will perform the review and analysis.

5. After any analysis is performed, a report of the findings will be forwarded to the Office of Human Resources. Human Resources will then meet with the Division of Security, the Bureau Chief (or designee) for whom the employee works, and/or outside entities to determine whether further action is warranted. In criminal cases, the Division of Security will coordinate the investigation with the appropriate law enforcement agency.
6. Violation of the Department's Computer System, Internet Code of Conduct and Computer Security Policy and/or the State of Connecticut Acceptable Use of State Systems Policy may result in disciplinary action up to and including termination.

Most violations of this Policy can be avoided by exercising good judgment and common sense. Any questions regarding this Policy should be referred to the Director of OIS for clarification.

(This Policy supersedes Policy Statement No. F&A-28 dated September 24, 2007.)



Jeffrey A. Parker
Commissioner

List 1 and List 3