CONNECTICUT DEPARTMENT OF TRANSPORTATION

POLICY STATEMENT

POLICY NO. F&A-28
September 5, 2018

SUBJECT: Connecticut Department of Transportation Policy on Computer Systems Acceptable Use

This Policy is put forth to Connecticut 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. Such persons are herein 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; Intranet access; USB devices; and handheld PDA devices (e.g., Blackberry) that combine computing, telephone, fax, Internet, Intranet 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 System's Policy (State Acceptable Use Policy) is posted at www.ct.gov/opm, and choose "Policies". **To be clear, all users are responsible for reading and complying with both the State Policy and this Department Policy.**

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 email, voicemail, and facsimile, including, but not limited to, emails sent or received on personal email accounts using State systems. The Electronic Monitoring Notice can be found on the State of Connecticut Office of Policy and Management website at https://www.ct.gov/opm/site/default.asp. Choose "Policies". Under "Technology", choose "Acceptable Use Policy". See "Additional Resources" for the Notice.

To re-emphasize: In addition to this Policy, the State Acceptable Use Policy applies to all users and failure to comply with the same may result in disciplinary action up to and including termination. The State Acceptable Use Policy can be found on the State of Connecticut Office of Policy and Management's website at www.ct.gov/opm, and choose "Policies".

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 (user ID) and user password. Users are required to take reasonable steps to prevent others from learning his/her user ID 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 material accessed or processed using his/her user ID 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 Department of Technology Service (DTS) to change user passwords, the password shall be changed every three months.

    c. Additions and deletions of user IDs and passwords from any system are the responsibility of the designated system administrator for that particular hardware system and/or software application. A form available on the

Department Intranet site is required for adding or deleting user IDs and passwords.

d. Unit managers and the Office of Human Resources must notify the Security Office and DTS Management or DTS Help Desk as soon as possible of the date when an employee will terminate employment. 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 DTS System Administrator for appropriate changes to the security level for the new position. This can be accomplished through an email to the DTS Help Desk.

2. Software Programs and Information residing on Department systems will not be disclosed or copied by users without appropriate authorization from DTS. Information released subject to Policy Statement No. EX.0.-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 DTS support staff with proper notification from the requestor, provided that proper approvals by the employee's manager and Director of DTS 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 DTS, with DTS 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 DTS Data Security Officer or at his/her direction. Installation of personally owned software on Department systems is strictly prohibited.

3. Cloud Computing Services – Cloud Computing Solutions: Any online cloud computing services or solutions will require the review of the Director of DTS and the approval of the State of Connecticut CIO prior to any requisition or purchase order.

4. Modems expose Department systems to network security concerns and, therefore, are prohibited unless specifically authorized by the Director of DTS. Alternative access methods will be considered by the DTS 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 DTS Help Desk.

5. 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 DTS.

5. Laptops and Tablets: All laptops and tablets must be encrypted with the encryption software approved by the State of Connecticut, Department of Administrative Services, Bureau of Enterprise Systems & Technology (BEST). Laptop and tablets specifications must be approved by DTS prior to purchase to ensure compliance with State and Department technology standards. Laptops and tablets 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 DTS Director approval, laptops and tablets with Microsoft Windows installed can replace desktop computers using connections previously approved and with proper security and encryption software installed by DTS. Upon request by DTS 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 DTS. 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 or tablets 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 DTS.

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 DTS 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 websites are blocked through Internet filtering, not every inappropriate site can be blocked due to the volatile nature of Internet information and search capabilities.

   BEST and DTS have the technical capability to proactively monitor Internet usage and view websites 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 DTS 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-DTS approved technology means (i.e., modems) is prohibited.

   c. The Internet is to be used and websites 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 websites for shopping, booking trips, research, etc.; downloading unauthorized software or inappropriate materials; Internet radio; chat room access; social networking sites (e.g., Facebook, Pinterest, Instagram, Twitter, etc.); and instant messaging programs (e.g., AOL Instant Messenger, MSN Messenger, and similar programs).

   d. Users shall not access, view, or otherwise connect with non-Department work-related websites; download, save, send, print, or email 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 DTS 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 DTS Management or DTS 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. The use of Social Media channels is subject to the State of Connecticut terms of use. The acceptable use policy can be found on the State of Connecticut Office of Policy and Management's website. Choose "Policies", then under TECHNOLOGY, choose "Social Media Policy".

i. 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: See the State Policy which can be found on the Connecticut State Office of Policy and Management's website at https://www.ct.gov/opm/site/default.asp. Choose "Policies", then "Security for Mobile Computing and Storage Devices". Individual bureaus are responsible for determining data that is confidential or restricted.

10. USB Flash Drives and Other Mobile Storage Devices must be purchased through the Department's purchasing approval process and are permitted for the portability and retrieval of non-confidential data only. Personal or non-State issued flash drives and other mobile storage devices are prohibited for use on Department systems. Such devices must not be bootable or used to launch applications. Users are responsible for the loss of removable devices and for safeguarding Department information at all times.

11. Personal Use: All Department systems, including State-issued computers, tablets and cell phones are a government resource and are subject to the same rules as other government resources. Use of the Department's computers, tablets and cell phones 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 email accounts (e.g., Gmail, Hotmail, Yahoo, etc.) to send or receive personal email; 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 (e.g., Facebook, Pinterest, Instagram, Twitter, etc.), and instant messaging programs (e.g., AOL Instant Messenger, MSN Messenger, and similar programs). Personally owned or non-state issued computer equipment and software including but not limited to Smartphones and Tablets are prohibited from being used with the Department's data communications network unless there is prior written authorization for business purposes only. Any such requests for authorization must be first submitted and approved by the employee's supervisor or manager and then forwarded to the IT Help Desk for final approval of the request.

12. Email: All email messages are considered the property of the State and, as such, are considered public records. Emails are not considered personal or private; therefore, users should have no expectation of privacy or confidentiality with regard to the same. All email messages are potentially accessible under the Freedom of Information Act. Any messages created, sent, received, accessed, or stored on Department systems constitute Department records. As such, any email, including any signature line/box, written by Department personnel should not, unless necessary for business reasons, include: (a) any declaration, testimonial, symbol or picture that makes a political or religious statement; (b) any message that is discriminatory or offensive to any protected class, or otherwise violates State and/or Department policies, or (c) any links to URLs or references to social media that include material which would be prohibited by (a) or (b). The State and the Department reserve the right to monitor (pursuant to Section 31-48d of the Connecticut General Statutes) and/or log email communications without further written notice. Email is stored on network backup tapes and is retrievable. The content and maintenance of a user's email account is the user's responsibility. This responsibility includes checking email daily and maintaining these public records as required under the "State Records Retention Schedule S1: Administrative Records". This schedule can be found on the Connecticut State Library's website at www.ctstatelibrary.org. Under Department links choose "Public Records Administration", then under "State Records Management Program" choose "General Records Retention Schedules", then "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 which can be found on the Connecticut State Library website. Emails should be retained according to this General Letter to ensure they can be retrieved. Users should also read and understand the "Electronic Mail Records Management Policy" (Policy ID: IT-REC-15-01), which is on the State Office of Policy and Management's website under "Policies". Users should also refer to the Department's record retention schedules for proper procedures regarding disposition of email communications and all correspondence must be maintained by subject as opposed to record type (i.e., if any of your emails are related to a construction project, these records must follow the retention period for that project). See CTDOT Policy No. F&A – 26 Records Retention which is on the Department's Intranet. **Important Note:** If any of your emails are subject to a litigation hold, those emails 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 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 Department systems are approved for DTS 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:

I. Alleged violations should be reported to the Office of Human Resources.

2. Human Resources, DTS 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 DTS 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 emails sent and received and internet usage. DTS 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 possibly 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 DTS for clarification.

(This Policy supersedes Policy Statement No. F&A-28 dated March 1, 2017.)

James Redeker
Commissioner