Revised December 1, 2017

LOUISIANA DEPARTMENT OF TRANSPORTATION AND DEVELOPMENT

SECRETARY'S POLICY AND PROCEDURE MEMORANDUM (PPM) NO. 51

SUBJECT: Use of Computers

EFFECTIVE DATE: July 22, 1996

INSTRUCTIONS: This memorandum supersedes all other memoranda and manuals.

1. INTRODUCTION

It is the policy of the Louisiana Department of Transportation and Development to fully comply with the Division of Administration's Office of Technology Services (OTS) policies and standards which are available at www.doa.la.gov/pages/ots/policies.aspx. The Louisiana Department of Transportation and Development (DOTD) owns and operates, through DOTD's Intelligent Trans System (ITS), various computer systems which are provided for use by employees in support of business activities. All users are responsible for ensuring that these systems and tools are used in a secure, effective, ethical and lawful manner. Access and privileges on other DOTD computing systems are assigned and managed by OTS system administrators of specific individual systems. Eligible DOTD employees may be granted access and privileges to a particular system or systems such that only those capabilities necessary to perform a job are granted. Users may not, under any circumstances, transfer these privileges to other individuals. The authorized user is responsible for the proper use of the system, including password protection. An ID, account and/or password is assigned to an individual and must not be used by anyone else. The individual to whom this is assigned is responsible for the proper use of this account. DOTD establishes this policy to ensure that DOTD/OTS issued computers are used for business-related purposes and to ensure that all communications are made in a professional manner. For purposes of this policy, "computer" is defined as a DOTD/OTS issued computers such as a desktop computer, laptop, tablet or phone. The use of DOTD/OTS resources, including electronic communications, should never be used inappropriately.

This policy sets forth regulations and requirements on the proper use of computers, servers, the intranet/internet, and the E-mail system; compliance with software licensing agreements and copyright laws; and the Division of Administration's Office of Information Services policies and standards.

2. USE OF COMPUTERS, WIRELESS DEVICES, AND OTHER COMPUTER DEVICES

A. Use and Care of Equipment. DOTD/OTS issued computers are to be used for official business purposes in furtherance of DOTD's mission; however, incidental limited personal use of DOTD/OTS computer resources is a privilege, not a right of employment, and must not interfere with DOTD business or employees' work performance, have an undue impact on the computer system and resources, nor violate any laws or DOTD/OTS policies. Limited personal use of DOTD/OTS

issued computers is a privilege that may be revoked at any time (Re Section 8. in this PPM). DOTD/OTS property and equipment is to be used responsibly and treated with appropriate care. Computers, software, and computer media such as USB Flash Drives, CD ROMS, etc., provided by the Department are the property of the State of Louisiana and are to be used exclusively for business-related purposes only by authorized personnel.

B. Viruses and Anti-Virus Software. Users of DOTD/OTS equipment are not permitted to copy, execute, or otherwise handle malicious or destructive programs such as computer viruses or worms. Any deliberate attempt by a user to infect DOTD/OTS assets, including computers, wireless devices, servers and networking equipment with a virus shall result in disciplinary action. All DOTD/OTS equipment must have installed and maintained an anti-virus program with current virus signatures. All incoming data, programs, and documents must be checked for viruses. If any DOTD/OTS equipment assigned to an individual becomes inadvertently infected, notification must be made immediately to the Office of Technology Services who will assist in the quarantine and removal of the virus. In addition, DOTD and the Office of Technology Services are responsible for reporting this to the OTS Chief Information Security Officer.

C. Removal of Data and Software. All DOTD/OTS equipment which has a hard disk drive and will be surplused or transferred to another section or agency must have all licensed software and data removed from the hard disk, including the operating system. Refer to the OTS Information Security Policy at http://www.doa.la.gov/Pages/ots/InformationSecurity.aspx for acceptable means of cleaning the hard drive. OTS employees can assist in the sanitization of hardware prior to surplusing.

D. Management of DOTD/OTS Issued Computers. All computers should be logged off and powered down at least once per week. This includes peripheral equipment, directly attached printers, speakers, scanners, etc. All computers must be configured based on the OTS computer policy. The OTS Chief Information Security Officer may grant exemptions on a case-by-case basis or because of an employee's job function. Refer to the OTS Security Policy at http://www.doa.la.gov/OTS/InformationSecurity/InformationSecurityPolicy-LA-v.1.0.pdf. Requests for exemption must be in writing to the OTS Agency Relationship Manager, signed by the section head or district administrator with adequate and complete justification for the exemption.

E. Assignment and Property Control of DOTD/OTS Issued Computers. All computer-related devices and peripherals issued by DOTD/OTS are the property and responsibility of OTS. In order for OTS to maintain accurate inventory and property control information, any movement or reallocation of equipment between DOTD employees must be performed by OTS. This includes moving equipment to a new

office or location or assigning equipment to a new user. An OTS Service Desk request must be initiated to change an assignment or location of all OTS property to ensure inventory records are updated accordingly. One of the following methods must be used to make the OTS Service Desk request:

- Email otssupport@la.gov
- Call (225) 219-6900 or Toll Free 1-844-219-6900
- Enter online at https://otssupport.la.gov

3. USE OF WIRELESS DEVICES, ACCESS POINTS, AND WIRELESS NETWORKS

A. Introduction. DOTD owns the airspace within the property boundaries of all DOTD sites. No department or individual may install wireless access points at or around any DOTD location on the DOTD/OTS Network infrastructure. A wireless network segment is more vulnerable to unauthorized access than a wired network. Wireless devices create additional exposure and vulnerability to the DOTD/OTS network and require enhanced protection from fraudulent use and eavesdropping. Wireless communication, which can include voice, video, and data, place an additional load factor on the DOTD/OTS network infrastructure. Implementation of these devices shall be aligned with the strategic direction of DOTD/OTS. DOTD/OTS allows guest wireless internet access to all wireless devices on all DOTD campuses statewide.

B. Security and Integrity of Wireless. Integrity and appropriate use of the wireless network must be ensured. Wireless devices and access points to the DOTD/OTS network are to be secured and authenticated in accordance with the OTS approved standard, currently primarily CISCO LEAP technology at DOTD. Access points will be installed by OTS based upon requirements for wireless connectivity and optimum placements of these devices. No wireless devices will be deployed within DOTD without specific authorization of OTS. Unauthorized rollouts of wireless networks or devices will be revoked from the DOTD/OTS network. Unapproved and non-standard units will be located and disconnected. All users of the wireless network must comply with DOTD/OTS policies and procedures including security and appropriate usage.

4. USE OF THE ELECTRONIC MAIL SYSTEM AND ELECTRONIC COMMUNICATIONS

A. Intended Use. All electronic communications including, but not limited to, E-mails and faxes are considered to be the property of DOTD and the State, not its employees, vendors or customers. All electronic communications and information transmitted by, received from, or stored in these systems are the property of DOTD and as such are intended to be used for business purposes only. Messages that are of only momentary communicative value need not be retained. Failure to routinely delete transitory messages can strain electronic storage resources. Use of E-mail is

a privilege, not a right. The E-mail systems are for use by all authorized DOTD employees to conduct the official business of the Department. Employees have no expectation of privacy as it relates to any information transmitted or received through E-Mail. This email policy additionally applies to employees using personal, password protected E-mail accounts, which are also subject to review and/or retrieval. DOTD/OTS reserves the right to access and monitor all messages transmitted or received through E-Mail or any form of electronic communication. Any request made pursuant to a subpoena or legal discovery or a public record request for E-Mail records must be referred to the DOTD General Counsel before the release of such records to the public.

Each authorized employee will be assigned a logon ID and password to access an E-Mail system. Employees are not allowed to originate E-Mail communications using another employee's ID.

E-Mail should be considered an alternative method of interdepartmental communication that may be monitored and reviewed at any level of the Department's management. Messages no longer needed for business purposes must be periodically archived or purged by users from their electronic message storage areas on the servers in accordance with DOTD Records and Retention Policies.

Electronic messages including but not limited to E-mail and faxes must not be used for illegal, disruptive, unethical or unprofessional activities, for personal gain or for any purpose that would jeopardize the interests of DOTD.

In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments. The current limit is 30 MB, which is set by the Office of Telecommunications Management (OTM).

B. Confidential Matters. Although electronic communications are protected by a person's confidential password, privacy is not guaranteed. Highly confidential, privileged or sensitive communications including Personally Identifiable Information (PII) should not be transmitted outside of the State's E-Mail system onto unsecured networks being managed by non-state carriers or internet providers.

Personally Identifiable Information refers to specific information that can be used to uniquely identify, contact, or locate a person or can be used with other sources of information to uniquely identify an individual. The concept of using PII to uniquely identify an individual is not new; however, it has become much more significant as Information Technology, and the Internet has made it easier to collect this data, leading to a profitable market in collecting and reselling this information for both legal and illegal purposes.

Examples of Personally Identifiable Information Data include:

- Full Name (when used in combination with items below)
- Social Security Number
- Vehicle Registration Plate Number
- Driver's License Number
- Credit Card Numbers
- Digital Identity
- Personal Computer IP Address
- Birthplace
- Birth date

In special cases when highly confidential, privileged or sensitive information or Personally Identifiable Information must be transmitted outside of the State's email system or network, the OTS Service Help Desk must be contacted at (225) 219-6900 or a service request must be submitted for assistance at https://otssupport.la.gov.

C. Personal Email Appearance Requirements

It is imperative that email transmitted within the DOTD maintain a consistent and professional look. Use of large personal logos, quotes, and personalized messages on signature lines often fail to maintain that professional look and also greatly increase the size of the email message which increases storage space expenses and reduces the efficiency of DOTD email systems.

When writing emails, plain text or rich text formats should be used as well as effective, clear, and descriptive subject lines. Emails should be written to be easily and quickly scanned by a reader by using lists, bullets, and spacing between paragraphs.

Simple fonts should be used such as Arial or Times New Roman. Script or complex fonts are not easy to read. Generally, black or dark blue color should be used to project the most readable and professional presentation.

A writer should refrain from using graphics and never use colorful backgrounds in an email. Flashing or animated graphics should not be used as these all detract readers from the message, prevent some readers from being able to easily view the message, and require the use of extra storage space on servers.

Emails should always include a complete and professional email signature. The signature should include full name, job title, Department of Transportation and Development, office telephone number, and email address. Email signatures should not include slogans, quotes, verses or other personal expressions or graphics.

Example signature:

- Name (Options: Bold, one font size larger than the title)
- Job title
- Department of Transportation and Development (options: one font larger than title, link to DOTD web site)
- Office: XXX-XXX-XXXX
- Fax: XXX-XXX-XXXX
- Cell: XXX-XXX-XXXX (optional)
- Email address

D. Use by Third Parties. The Department's E-Mail system may be used by consultants and other third parties as approved by the Undersecretary of Management and Finance. Third parties may only use the Department's E-Mail systems if they agree to abide by all applicable rules.

5. USE OF WEB PUBLISHING SERVERS AND THE INTERNET/INTRANET SYSTEMS

The use of DOTD equipment to establish data communications with the Internet/Intranet will be subject to the following requirements:

A. No computer or other devices will be configured as any server (FTP, TELNET, WWW, etc.) without written approval. The user's supervisor will provide a written justification approved by their respective section head and directorate. Review and approval of this justification must be obtained from OTS via the OTS Agency Relationship Manager before any device is configured as a server.

B. The DOTD Public Information Office is responsible for monitoring all information published on the DOTD websites. (The websites include the DOTD intranet and the DOTD internet.) The DOTD Public Information Office may delegate to Section Heads, District Administrators or other Appointing Authorities the responsibility to review and authorize the content published on their respective areas of the site. The Section Heads, District Administrators or other Appointing Authorities may select a knowledgeable Web Content Manager(s) for updating their respective areas of the site. The Web Content Manager(s) with knowledge of the content must be approved by the Section Head/District Administrator, Office Head and the Secretary's Office. After approval, the Web Content Manager(s) must be trained by OTS prior to being granted access to update the websites. The Public Information Office has overall authority to remove content if deemed necessary as well as manage a consistent appearance of the site.

The Headquarters Human Resources Section shall have the responsibility to monitor and review bulletin board postings to the DOTD intranet website to ensure

that the content adheres to established guidelines. The Headquarters Human Resources additionally has the responsibility to have inappropriate postings removed.

C. The Office of Technology Services will define the installation procedure for software and perform all TCP/IP installations for all equipment connected to the DOTD Data Communications Network. Certain networking devices or equipment used for specific ITS purposes on ITS Networks may also be defined and configured by the ITS Section in coordination with OTS.

D. The employee is responsible for the security of his/her computer and the proper use of the Internet. The employee's supervisor is responsible for monitoring the employee's use of and the Internet to ensure professional and job-related use.

E. Users must use the enterprise anti-virus program to scan for potential software viruses.

F. Employees accessing the Internet are representing the Department. All communications should be for business reasons. Employees are responsible for using the Internet in an effective, ethical, and lawful manner.

G. The Internet should not be used for personal gain or the advancement of individual views. Solicitation of non-department business or any use of the Internet for personal gain is strictly prohibited. Use of the Internet must not impact the operation of the Department's data communication network. It must not interfere with employee productivity. The Internet may not be used for illegal or unlawful purposes including but not limited to copyright infringement, obscenity, libel, slander, fraud, illegal gambling, intentional spreading of viruses or computer tampering.

H. All messages/notes created, sent or retrieved from the Internet are the property of the Department, and employees have no expectation of privacy in any information sought or transmitted through the use of the Internet. The Department reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate.

6. COPYRIGHTED/PATENTED MATERIALS

Employees must abide by the terms of all software licensing agreements and copyright laws. Employees are not to duplicate or download any software or materials that are copyrighted or patented. (This policy also applies to "shareware" products.) Employees are to follow the procedures outlined in PPM No. 42, Acquisition of all Computer-Related Technologies, including Hardware and Software, if there is a need to install employee-owned software and/or equipment.

7. COMPUTER MONITORING

Electronic communication systems (voice mail, E-mail, and fax) and all messages generated on or handled by electronic communications, including back-up copies, are considered to be the property of DOTD and are not the property of the users of the electronic communication services. Internet/Intranet, E-Mail or other on-line communications, and the material stored on any DOTD/OTS computer, including computer hard drives and other media such as CD ROM's, USB Flash Drives, etc., are not privileged or private. This lack of privacy extends to anything the employee creates, receives, prints or sends on the Department's paper or electronic documents such as E-Mail, printers or other information systems.

If anyone reports indications of illegal activity or violations of Department policy or security, the Department will investigate and take appropriate disciplinary action. In the course of an investigation, the Department may inspect the contents of E-Mail communications and material stored on any DOTD/OTS computer, including computer hard drives and other media such as USB Flash Drives, CD ROM's, etc. Employees shall not delete the alleged offending/illegal information until any investigation is complete. Auditors will routinely inspect this same material in the course of an audit.

The Office of Technology Services is responsible for servicing and protecting its electronic communications networks and systems.

8. MISCELLANEOUS USE AND RESTRICTIONS

A. Personal Use. The Department recognizes that occasional personal use of the Internet and Department's computer system may occur. While not encouraged, such occasional personal use is tolerated provided such:

(1) Is incidental, brief, occasional and intermittent;
(2) Does not result in additional cost to the Department or the State;
(3) Does not interfere with performance of the employee's job duties;
(4) Does not impact system-wide usage;
(5) Does not circumvent security systems;
(6) Is not intended to produce personal monetary gain;
(7) Is not offensive, profane, or otherwise inappropriate;
(8) Does not violate the prohibitions of this policy or any federal, state, or local law or regulations; and or
(9) Must occur before or after work hours, official breaks, or lunch period

9. ENFORCEMENT/VIOLATIONS

Violations of any guidelines listed above may result in appropriate disciplinary action, up to and including termination. Failure to observe copyright or license agreements may also result in legal action by the copyright owner.

Shawn D. Wilson, Ph.D.
Secretary