Approved:

Effective: April 2, 2020
Review: August 23, 2019
Office: Information Technology
Topic No.: 325-060-020

Department of Transportation

SECURITY AND USE OF INFORMATION TECHNOLOGY RESOURCES

AUTHORITY:

Sections 20.23(3)(a), and 334.048(3) Florida Statutes (F.S.)

REFERENCES:

Chapter 60GG-2, Florida Administrative Code (F.A.C.)
Chapter 119 and Section 282.318, Florida Statutes (F.S.)

PURPOSE:

The purpose of the Security and Use of Information Technology Resources is to provide information on the use of the Department of Transportation's (Department) information technology resources and its security extending to all members of its workforce, as well as those who access, process, or have custody of data.

SCOPE:

This procedure applies to all members of the Department's workforce, as well as those who access, process, or have custody of data and is set into place to protect the Department's assets from misuse, abuse, and loss through the management of a comprehensive information technology resources security program.

1. GENERAL REQUIREMENTS

It is the policy of the Department to protect information and information technology resources as strategic assets. Information technology resources include computer hardware and devices (such as desktop computers and workstations, mainframe computers, notebooks, tablets, or laptop computers, and mobile devices such as smart phones), software, networks, connections, applications (including Web applications and E-mail), cloud services (such as

Software as a Service, Platform as a Service, Infrastructure as a Service), and data. These resources may be owned, leased, or contracted services of the Department. This procedure applies to all members of its workforce. Further, this procedure applies to all Department information technology resources that access, process, or have custody of data.

1.1 The Department's Chief Technology Officer (CTO) is responsible for administering the Department's data and information technology resources program. The Secretary will designate an Information Security Manager (ISM) to assist the CTO in administering the information technology resources security program. The ISM or designee shall be granted access to monitor all agency information technology resources. All offices within the Department that develop, maintain, or support, computer systems shall coordinate any required security efforts with the ISM. Offices shall designate computer security coordinators. In addition to the requirements of ***Chapter 60GG-2, F.A.C.,*** the ISM, Inspector General, or other specifically authorized personnel shall be granted access to review audit logs containing accountability details.

1.2 The Department's information technology resources security program involves the following areas:

(1) Confidentiality of Information and Data
(2) Control of Information Technology Resources
    a. Electronic Mail
    b. Internet
    c. Social Media Sites
    d. Hardware and Software
(3) Physical Security and Access to Data Processing Facilities
(4) Logical and Data Access Controls
(5) Network Security
(6) Protection Against Loss
(7) Compliance

1.3 This procedure applies to all Department information technology resources that access, process, or have custody of data. This includes all owned, leased, and contracted services involving mainframe, distributed processing, and networking environments. Department information technology resources are intended to be used for Department business.

1.4 Each individual accessing Department information technology resources is expected to use good judgment and common sense to avoid abuse and inappropriate use of resources. For example, it is inappropriate to use any resource in a manner which will interfere with the timely performance of an individual's normal work duties, adversely impact the performance of the resource or unnecessarily increases the cost of the resource, cast disrespect or adverse reflection upon the Department, reduce public confidence, support a personal business, support political or religious activities, or detract from the Department's routine functions. Furthermore, employees shall not access, send, store, create, or display inappropriate

materials including, but not limited to, gambling; illegal activity; sexually oriented materials; nudity; or materials that include profane, obscene, inappropriate, or discriminatory language.

1.5 Each individual with authorized access to Department information technology resources shall be responsible for appropriately maintaining systems security. All users are required to comply with all controls established by information technology resource owners and custodians, protect confidential information against unauthorized disclosure, and protect the Department from unauthorized access to information resources, including any connections to the Department network.

1.6 Each individual is required to comply with the terms and conditions of any license or copyright.

1.7 Each individual who has been granted privileged or specialized security authorizations is considered to be in a position with trusted security requirements. This includes, but is not limited to, individuals who grant security authorizations, administer networks and servers, use voice and telecommunications diagnostic equipment, use remote control software, migrate software and code from test to production environments, or perform other security-related activities deemed critical by their manager or supervisor. The Data Owner shall be responsible for the proper training of each individual who has been granted access to confidential and exempt data and information according to ***Section 2*** of this procedure.

1.8 Each individual is required to immediately report any breach of security, including but not limited to, unlawful accesses, suspected intrusions, theft, or other actions that compromise the security of information technology resources to the FDOT Service Desk and all other appropriate on-call staff in the event the suspected breach occurs outside normal business hours. Additionally, Computer Security Incident Response Team personnel, as designated in ***Chapter 1*** of the ***Transportation Technology Manual***, ***Topic No.: 325-000-002,*** must report computer security incidents to the Division of State Technology and the Cybercrimes division of the Florida Department of Law Enforcement.

1.9 Each individual with authorized access to the Department's information technology resources shall follow this procedure and all information security standards and procedures. Any request for a change or exception to this procedure shall be submitted via the ***Information Resource Request (IRR)*** system for approval by the Information Security Manager. Requests for exceptions to this procedure that are of a confidential nature shall not be submitted through the IRR system, and shall be instead directed to the Department's Information Security Manager. The IRR system shall not include any information or documentation that is confidential or exempt from the inspection and copying provisions of Florida's Public Records Law. Questions regarding whether a particular document contains confidential or exempt information shall be directed to the Office of General Counsel.

1.10 Misuse or abuse of any information technology resource, including e-mail, Internet access, and social media sites by any member of the Department's workforce may result in the

revocation of access, and other disciplinary actions up to, and including dismissal, termination of contracts, or other legal action. All users are on notice that state or federal law may impose criminal penalties for certain computer related acts that may also constitute violations of this procedure.

2. CONFIDENTIALITY OF INFORMATION AND DATA

2.1 Confidential and exempt data and information must be made readily identifiable by the owner and treated as confidential in its entirety. Information systems access shall be limited to individuals having an authorized need to use the information. Data file and program access will be limited to those individuals authorized to view, process, or maintain particular systems.

2.2 Data marked confidential should not be publicly released prior to consultation with the Office of General Counsel.

2.3 "Sensitive" agency-produced software are those portions of data processing software, including the specifications and documentation, which are used to:

- Collect, process, store, and retrieve information that is exempt from ***Section 119.07(1), F.S.***;
- Collect, process, store, and retrieve financial management information of the agency, such as payroll and accounting records; or
- Control and direct access authorizations and security measures for automated systems.

2.4 Confidential and exempt data and information must be encrypted when stored (at rest) and when sent (in transit). E-mail communication sent between Department employees and consultants (all having an @dot.state.fl.us email address) are encrypted at rest and during transmission. Communication with e-mail recipients outside the Department might not be encrypted. Users shall not transmit confidential and exempt data or information to external recipients through the e-mail system. Users transmitting confidential and exempt data or information to external recipients shall use an appropriate and approved encrypted technology, such as the Department's File Transfer Appliance (FTA).

2.5 While the Department expects users to adhere to the requirements regarding confidential and exempt data and information, users should have no expectation of privacy since the data they create or receive on the state network system is the property of the State of Florida and is subject to ***Chapter 119, F.S.***

3. CONTROL OF INFORMATION TECHNOLOGY RESOURCES

3.1 ELECTRONIC MAIL (E-MAIL)

3.1.1 Employees are granted use of e-mail to carry out the mission of the Department and to promote efficiency and improved communications with our internal and external customers.

E-mail should be used for business purposes. Any personal use of e-mail must be brief, infrequent, and in compliance with the expectations described in ***Section 1.4*** of this procedure. E-mail is authorized through the Department's official e-mail and Internet applications. The transmission of Department business related e-mail to a personally owned e-mail address is prohibited. Authorized users must not use personal e-mail accounts to conduct Department business. Users of the Department's e-mail system shall not enable rules to auto-forward e-mails and calendar appointments to external e-mail addresses.

3.1.2 The Department will conduct random reviews of e-mail, through direct access or the use of archival data, to detect abuse or misuse of these resources, without notice to employees. E-mail messages are automatically archived upon receipt. Deleting an email from the inbox does not delete the email from archives. E-mail is not private and is subject to the requirements of ***Chapter 119, F.S.***

3.1.3 Use of a non-departmental e-mail system (i.e., Gmail, AOL, Yahoo-mail) through the Department's network is prohibited.

3.2 SOCIAL MEDIA SITES

3.2.1 The Public Information Office is responsible for administering the Department's social media outreach program and establishing the Department's social media accounts.

3.2.2. Access to social media sites such as YouTube, Facebook, Instagram, and Twitter is provided for business purposes. Members of the Department's workforce shall not post content related to Department business, except through Department approved accounts, subscription logon credentials or an approval from a Communications Manager. Employees are permitted to repost official Department posts to their personal social media accounts without altering the contents of the original post.

3.2.3. Any personal use of social media sites must utilize personal account credentials that are not affiliated with the Department. Access to personal accounts must be brief, infrequent, and in compliance with the expectations described in ***Section 1.4*** of this procedure.

3.2.4. Authorized agents who are administering social media sites on behalf of the Department must also adhere to these guidelines.

3.2.5. The Department's Social Media Guide should be referenced when creating, posting, and retaining social media content on behalf of the Department. The purpose of this document is to ensure consistency in messaging, retention of public information and security when using online accounts.

3.3 HARDWARE AND SOFTWARE

3.3.1 All computer hardware and software used by members of the Department's workforce in

the performance of their duties shall be Department owned or leased unless specifically approved by exception from the ISM via the IRR system.

3.3.2 If an exception is approved, it is the responsibility of the equipment owner to implement appropriate security controls to safeguard their equipment. The Department will not provide support for non-Department owned or leased hardware or software, and will not be liable for any damage resulting from connectivity to Department information technology resources.

3.3.3 Only authorized personnel will use software that allows observation or control of a remote computer. Remote control will be used for the sole purposes of testing, systems maintenance, troubleshooting, and user support. This software must provide an “acceptance” or “notification” mechanism to a remote user informing them that their computer is under remote control.

3.3.4 With the exception of peripheral equipment, such as headsets, speakers, and microphones, users may not install personal hardware or software on Department equipment.

3.3.5 Illegally exporting software, technical information, encryption software, or technology may result in criminal or civil penalties.

3.3.6 Games or entertainment software may not be used on Department owned or leased machines. As technology permits, all gaming and entertainment portions of an authorized software package shall be removed upon installation.

3.3.7 When it is beneficial to the State and approved in advance by the employee's supervisor or higher management, Department owned or leased computers may be used for educational and training purposes for the following programs or related courses:

1. Certified Public Manager (CPM);
2. Educational Leave With Pay (ELWP); and
3. Any course that meets a work-related need as determined by the supervisor, including courses taught by or for the Department.

This does not include tuition waiver courses taken by employees at a state university.

3.3.8 This procedure shall not be construed to prohibit the authorized evaluation of hardware, software, or new technologies.

4. PHYSICAL SECURITY AND ACCESS TO DATA PROCESSING FACILITIES

4.1 Information shall be created and maintained in a secure environment. The cost of security shall be commensurate with the value of the information, considering value to both the Department and to a potential intruder. Measures, with respect to the creation and maintenance of information, shall be taken to prevent the unauthorized modification, destruction, or disclosure of information by any person, at any location, whether accidental or intentional. Additional safeguards shall be established to ensure the integrity and accuracy of

Department information that supports critical functions of the Department, and for which processing capabilities must be provided in the case of a disaster, and for those information assets with which the Department has entered into a data or information sharing agreement.

4.2 Removal of panels, partitions, or other equipment at any workstation is prohibited. The removal of such equipment shall only be done by authorized personnel for the purposes of maintaining the Department's information technology resources.

5. LOGICAL AND DATA ACCESS CONTROLS

5.1 Access to, and use of, the Department's information technology resources is authorized for a specific individual and must be used exclusively by that individual. This access is managed by the assignment of authentication controls to each authorized individual who needs access to the Department's information technology resources.

5.2 Access passwords shall neither be shared, nor entered via any automatic means, such as macros, and shall be unreadable during transmission and storage using appropriate encryption technology. Additionally, members of the Department's workforce are responsible for safeguarding their passwords and other authentication controls against accidental or intentional disclosure and must refuse the receipt of another user's assigned authentication controls. Examples of authentication controls include: passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

5.3 Passwords which prevent workstations from booting or powering up shall not be used on any Department owned or leased workstation.

5.4 Controls shall be established to maximize the accuracy and completeness of data.

5.5 Adequate separation of functions must be maintained to help prevent fraud or other unauthorized activity. Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless the data has been scrubbed or unless all personnel involved in testing are otherwise authorized access to the data. Exempt data in the production environments shall not be used for development.

5.6 Systems documentation shall be maintained by the information owner and shall be made available to the ISM, Inspector General, and other authorized personnel upon request.

5.7 System security plans shall be maintained by the information owner and stored on the Security Assessment and Authorization SharePoint site. System security plans are considered confidential per ***Section 282.318, F.S.,*** and shall only be made available to those individuals with a business need to view, process, or maintain the plan. Requests for access to system security plans will be managed by the ISM with approval from the information owner.

5.8 After a new system has been placed in operation, an updated system security plan shall be approved by the ISM if there are program changes to the system such as access, authentication methods, or data connections.

5.9 Default passwords, including those supplied by vendors, are not permitted for use and must be changed where technology permits, and as soon as technically feasible.

5.10 Mobile computing devices shall be issued to, and used only by, authorized users. Mobile computing devices shall require user authentication.

5.11 A sufficiently complete history of transactions shall be maintained for each session involving access to critical information to permit an audit of the system by tracing the activities of individuals through the system.

6. NETWORK SECURITY

6.1 Computer hardware shall not establish simultaneous network connections between a Department network and any other non-Department network. Unauthenticated access is prohibited.

6.2 Any request to connect an external network to the Department's data communications network must be documented and approved specifically with an ***Information Resource Request*** in accordance with ***Chapter 7*** of the ***Transportation Technology Manual, Topic No.: 325-000-002*** by the Chief Information Officer (CIO) or Designee and the Department's ISM. Before connecting, appropriate security controls, such as firewalls, must be implemented to protect the Department's network from unauthorized access.

6.3 Only individuals authorized by the ISM or CIO can use voice and data telecommunications diagnostic hardware and software, such as communications line monitors. Use is restricted to testing, monitoring, and troubleshooting, unless specifically authorized in writing by the ISM or CIO for other business-related activities.

6.4 Technology managers shall monitor technology resources to ensure desired performance and facilitate future capacity-based planning. Technology managers shall ensure regular review of system activity logs. Technology managers shall ensure regular review of system, security, and application activity logs. Events which indicate a security concern shall be investigated and the results of the investigation shared with the agency ISM.

6.5 Access to the Department's information technology resources shall be granted based on the principles of least user privilege and need to know.

6.6 Members of the Department's workforce shall use Department provided storage locations as documented in the Department's ***Technology Resource Standards*** for the storage of Department created, owned, and managed data.

7. PROTECTION AGAINST DATA LOSS

7.1 Where technology permits, all Department owned, leased, or managed computers, servers and mobile computing devices must have an anti-virus software/anti-malware program installed, operating, and appropriately updated at all times.

7.2 The Department provides anti-virus software and distributes updates for Department owned, leased, and managed devices. Appropriate configurations include real-time protection to support ongoing or background scans upon the execution of a "create, open, move, copy, or run" command. OIT is responsible for appropriate configuration for this software and no user shall alter this configuration. The anti-virus software is identified in the ***Technology Resource Standards.***

7.3 Individuals choosing to use personally owned devices to conduct Department business must have an approved AARF request for Personal Device Access and have on file a signed ***Acceptable Use Agreement, Topic No. 325-060-08***, available on the Department's ***Forms and Procedures*** Intranet site.

7.4 Only outside electronic data, software, or documents that have been approved for use by the Department are permitted. In all instances, electronic media, such as data, software, and documents, must be scanned for viruses before being used or accessed on a Department computer. It is the responsibility of vendors, consultants, and contractors to ensure that electronic media provided to the Department is free from malware, is safe for use, and does not compromise the integrity, confidentiality, or availability of the Department's information technology resources.

7.5 Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location. The security controls over the backup resources shall be as stringent as the protection required of the primary resources.

7.6 All information technology resources identified as critical to the continuity of governmental operations shall have written and cost effective contingency plans to provide for the prompt and effective continuation of critical state missions in the event of a disaster. Contingency plans shall be tested at least annually.

7.7 Each agency application or system with a Federal Information Processing Standards (FIPS) 199 categorization, which is hereby incorporated by reference, of moderate impact or higher shall have a documented system security plan.

7.8 Members of the Department's workforce shall logoff or lock their workstations prior to leaving the work area.

7.9 All workstations shall be secured with a lock screen timeout with the automatic activation set at no more than 15 minutes.

7.10 Except for assigned Department mobile devices, removal of Department owned, managed, or leased information technology resources requires documented approval from the information resource owner.

7.11 The Department shall monitor for unauthorized information technology resources connected to the agency internal network.

7.12 Strong encryption shall be enabled on agency owned mobile devices, removable media, and workstations.

8. CLOUD SERVICES

8.1 The Department has selected Microsoft's Office 365® platform to enhance collaboration with internal and external customers, improve productivity, provide greater accessibility to information and data, and to promote continuity in the Office of Information Technology's service offerings. Microsoft Office 365® includes the following applications: Office Suite (Outlook, Publisher, Word, Excel, Power Point, Access, and OneNote), SharePoint, and Skype. Office 365® improves accessibility to information and data through an online portal. As such, data and information created locally on a Department owned, managed, or leased information technology resource may be accessed from an online portal. While improved accessibility can create efficiencies, it also introduces additional risk. To protect the Department's data and information from unauthorized access and modification, members of the Department's workforce shall adhere to the following minimum-security requirements:

1. When sharing content via OneDrive, use folders to share groups of files with others; only share files with specific individuals, never with 'everyone' or the public.
2. Confidential data and information stored in OneDrive and SharePoint online shall follow the Department's policy and governance as an extension of internal Technology Resources.
3. Members of the Department's workforce who use OneDrive to share data and information shall remove sharing privileges when such privileges are no longer needed.
4. Members of the Department's workforce shall only synchronize files on machines that are owned, leased, or managed by the Department.
5. Members of the Department's workforce shall not store information and data unrelated to the Department on OneDrive.

8.2 Although Office 365® promotes accessibility of information and data via the online portal, members of the Department's workforce shall not access the online portal from untrusted sources including both computers and networks. Members of the Department's workforce shall only access information and data through the online portal if the workforce member trusts that both the computer and the network are free from malware and are running an anti-virus program.

9. TRAINING

None.

10. FORMS

Acceptable Use Agreement, Topic No. 325-060-08