



Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

ANANTH PRASAD
SECRETARY

POLICY

Effective: December 5, 2012
Office: Information Systems
Topic No.: 001-325-060-f

SECURITY AND USE OF INFORMATION TECHNOLOGY RESOURCES

1. GENERAL REQUIREMENTS

It is the policy of the Department of Transportation (Department) to treat information and information technology resources as strategic assets and to protect those assets from misuse, abuse, and loss through the management of a comprehensive information technology resources security program. 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 and Blackberries), software, networks, connections, applications (including web applications and e-mail), and data.

1.1 The Department's Chief Information Officer (CIO) 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 CIO in administering the information technology resources security program. All offices within the Department that develop computer systems shall coordinate any required security efforts with the ISM. Offices may designate computer security coordinators.

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

- (1) Confidentiality of Information & 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 policy 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, microcomputer, 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 explicit materials, or materials that include profane, obscene or inappropriate language, or discriminatory, racial, or ethnic content.

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, for protecting confidential information against unauthorized disclosure, and for protecting 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 that applies to the use of any software used for Department business.

1.7 Each individual that 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 that 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.

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. Additionally, responsible personnel as designated in the **Computer Security Incident Response Team, Topic No. 325-060-015** must report computer security incidents to the AEIT-OIS.

1.9 Each individual with authorized access to the Department's information technology resources shall follow this policy and all information security standards and procedures. Any request for a change or exception to this policy shall be submitted via e-mail to the Chief Information Officer.

1.10 Misuse or abuse of any information technology resource, including e-mail, Internet access, and social media sites, may result in access being revoked and disciplinary action for Department employees, up to and including dismissal. Misuse or abuse of Department information technology resources by contractors, consultants, or other persons may result in revocation of access, 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 policy.

2. CONFIDENTIALITY OF INFORMATION AND DATA

2.1 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 Confidential information or confidential data is information not subject to inspection by the general public under state or federal law, rule, or regulation. Confidential information and confidential data must be made readily identifiable by the owner and treated as confidential in its entirety.

2.3 "Sensitive" agency-produced software is 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.

A sufficiently complete history of transactions associated with the use of sensitive software will be maintained, as determined by risk analysis and technical feasibility, to permit an audit of the use of the software.

2.4 Confidential data or confidential information must be encrypted before being transmitted over a network. Currently, Department e-mail is not encrypted and therefore users should not transmit confidential data or information through the e-mail system. Additionally, encryption must be enabled on information technology resources to include but not be limited to desktop computers, notebooks/laptops, servers, smart phones, Blackberries, thumb drives, etc. that store or are used to transport confidential data, or confidential information, or both.

2.5 While the Department expects users to adhere to the requirements regarding confidential data and confidential 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 the requirements of **Chapter 119, Florida Statutes, Public Records**.

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 policy. E-mail is authorized through the Department's official e-mail and Internet applications. In cases where personal e-mail accounts are utilized for Department business purposes, copies of any e-mail must be forwarded to an official Department e-mail account. (**Note:** Accessing non-departmental e-mail systems through the Department's network is prohibited. See **Section 3.1.3** of this policy.)

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 is archived, even when an employee deletes it from their file. E-mail is not private and may be subject to the requirements of **Chapter 119, Florida Statutes, Public Records**.

3.1.3 Use of a non-departmental e-mail system (i.e., AOL, MSN, Yahoo-mail) through the Department's network is prohibited unless it is specifically approved with an **Information Resource Request, Form No. 325-005-01** in accordance with **the Acquiring Information Technology Resources Procedure, Topic No. 325-080-001**.

3.2 INTERNET

3.2.1 Employees are granted use of the Internet to carry out the mission of the Department and to promote efficiency and improved communications with our internal and external customers. The Internet should be used for business purposes. Any personal use of the Internet must be brief, infrequent, and in compliance with the expectations described in **Section 1.4** of this policy. Internet access is only authorized through the Department's proxy server unless specifically approved and documented by the ISM.

3.2.2 OIS will maintain detailed records of all Internet usage for use in detecting abuse or misuse of this resource without notice to employees.

3.3 SOCIAL MEDIA SITES

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

3.3.2. Access to social media sites such as YouTube, Facebook, and Twitter is provided for business purposes. No employee may post content related to Department business, except through Department approved accounts and subscription logon credentials.

3.3.3. 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 policy.

3.4 HARDWARE AND SOFTWARE

3.4.1 All computer hardware and software used by Department personnel in the performance of their duties will be Department owned or leased. Exceptions for special circumstances may be approved with an **Information Resource Request, Form No. 325-005-01** in accordance with the **Acquiring Information Technology Resources Procedure, Topic No. 325-080-001**.

3.4.2 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.

3.4.3 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.

3.4.4 A user may not install personal hardware or software on Department equipment unless it is specifically approved with an **Information Resource Request, Form No. 325-005-01**, in accordance with the **Acquiring Information Technology Resources Procedure, Topic No. 325-080-001**.

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

3.4.6 Under no circumstances will game or entertainment software be used on Department owned or leased machines unless it is specifically approved with an **Information Resource Request, Form No. 325-005-01**, in accordance with **Acquiring Information Technology Resources Procedure, Topic No. 325-080-001**. As technology permits, all gaming and entertainment portions of an authorized software package must be removed immediately.

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

- Certified Public Manager (CPM);
- Educational Leave With Pay (ELWP); and
- 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.

3.4.8 This policy 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, will be taken to ensure against the unauthorized modification, destruction, or disclosure of information by any person, at any location, whether accidental or intentional. Safeguards will 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.

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 assigning authentication controls, a unique userid and password, 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. The users to whom passwords are assigned shall protect the passwords from disclosure and must refuse the identification of all other user's passwords.

5.3 Passwords which prevent workstations from booting or powering up shall not be used on any Department owned or leased microcomputers or workstations without specific OIS approval, documentation and control.

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 desensitized or unless all personnel involved in testing are otherwise authorized access to the data.

5.6 After a new system has been placed in operation, all program changes shall be approved before implementation to determine whether they have been authorized, tested, and documented.

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

6. NETWORK SECURITY

6.1 Computer hardware shall not establish simultaneous network connections between a Department network and any other non-Department network unless it is specifically approved with an ***Information Resource Request, Form No. 325-005-01***, in accordance with the ***Acquiring Information Technology Resources Procedure, Topic No. 325-080-001***. 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 by the CIO. 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 CIO for other business related activities.

6.4 Information technology resources users shall be granted access to information technology resources based on the principles of least user privilege and need to know.

7. PROTECTION AGAINST LOSS

7.1 Where technology permits, all leased or managed computers, servers and mobile computing devices connected to the Department's network must have an anti-virus software 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. No user shall alter this configuration. The anti-virus software is identified in the ***Information Technology Resource Standards, Topic No. 325-080-050***.

7.3 Individuals choosing to use personally owned devices to conduct Department business must receive approval and agree to sign and comply with the ***Request to Use Personally Owned Computer Mobile Computing Device, Topic No. 325-060-20 Form***, available on the Department's Infonet 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 on a Department computer. It is the responsibility of vendors, consultants, or contractors to ensure that electronic media provided to the Department is not infected. Infected electronic media will be returned.

7.5 Data and software essential to the continued operation of critical agency functions shall be backed up. The security controls over the backup resources shall be as stringent as the protection required of the primary resources.

7.6 All information 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 Department computer users shall logoff or lock their workstations prior to leaving the work area.

7.8 All workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.



Ananth Prasad, P.E.
Secretary