OFFICE OF INFORMATION TECHNOLOGY MANUAL

2023-2024

TABLE OF CONTENTS

INTRODUCTION

OFFICE OF INFORMATION TECHNOLOGY MANUAL

PURPOSE:

The ***Office of Information Technology Manual (OIT Manual)*** contains the standards, procedures, and requirements related to information technology resources. Information and technology resources are strategic and vital assets that enable the Department to meet its mission. This OIT Manual ensures consistency and efficiency for the proper acquisition, security, use, distribution, and disposal of information and Information Technology resources.

AUTHORITY:

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

SCOPE:

This OIT Manual must be followed by all users of the Department's information technology resources. It applies to all Central Office and District units within the Florida Department of Transportation.

REFERENCES:

Enterprise Business Glossary

CHAPTER 1

GENERAL INSTRUCTIONS

1.1 STATUTORY AND RULE COMPLIANCE

All users of FDOT's information technology resources are required to:

1.1.1 Comply with all requirements of Florida Administrative Code Chapter 60GG: Florida Digital Service.

1.1.2 Comply with all applicable Florida Statutes.

1.1.3 Comply with all other laws, rules, and/or regulations outlined by the state or federal government.

1.1.4 Comply with all policies, procedures, and standards outlined in this OIT Manual.

1.1.5 Comply with all licensing requirements and copyrights.

1.2 FDOT INFORMATION TECHNOLOGY RESOURCES

1.2.1 FDOT information technology resources are to be used for business purposes only.

1.2.2 Computing devices used for Department business must remain compliant with all requirements of the *Security and Use of Information Technology Resources (SUITR)*, *Topic No. 325-060-020*.

1.2.3 The System Microsoft Endpoint Configuration Manager (MECM) will be the source for software updates, deployment, and reporting for all managed systems.

1.2.4 Software installed by the local district IT staff will be the local district's responsibility.

1.2.5 Windows Server Update Services (WSUS) will be used for patching of unmanaged systems.

1.2.6 All data and software essential to the continued operation of critical agency functions shall be backed up locally and mirrored to an off-site location.

1.3 MOBILE DEVICE MANAGEMENT

This section defines the requirements for managing mobile devices with endpoint protection.

1.3.1 All staff assigned a department issued cell-enabled device are responsible for ensuring the device is in compliance with the Department's *Text Messaging Policy, Topic No. 001-325-067*.

1.3.2 Computing devices that cannot run Mobile Device Management (MDM) are not permitted to connect to the FDOT network without an approved exception Letter of Authorization.

1.4 FDOT SERVICE DESK

1.4.1 The FDOT Service Desk, managed by Central Office, OIT, is the only Service Desk authorized for use in requesting technology service and support for the Department. This includes but is not limited to, computer hardware, software, and application development services.

REFERENCES:

Security and Use of Information Technology Resources (SUITR), *Topic No. 325-060-020*
Text Messaging Policy*, Topic No. 001-325-067*
Software Updates Deployment Method & Practice
Backup Data Rules & Requirements Method &Practice

CHAPTER 2

EXCEPTIONS

This chapter outlines the requirements for requesting exceptions to Office of Information Technology (OIT) policies, procedures, and standards (including those outlined in this Manual).

2.1 EXCEPTION REQUESTS

2.1.1 All exception requests must be submitted through the information resource request system, which will serve as the sole entry point for those requests.

2.2 AUTHORIZATIONS

2.2.1 Exceptions are only valid upon receipt of a Letter of Authorization (LOA) issued by CIO or delegate.

2.2.2 All exception approvals are conditional upon any compensating controls listed in the LOA.

2.2.3 An LOA is revocable at any time if the compensating controls are not met or there is a change in strategic or executive direction.

2.3 EXCEPTION APPROVAL TIME LIMITS

2.3.1 Exceptions may be granted for a maximum period of one (1) year.

2.3.2 Renewals may be granted by CIO or delegate.

2.4 APPROVED EXCEPTION VERIFICATION REVIEWS

2.4.1 Anyone with an approved exception must comply with all Exception Verification and Quality Assurance Review (QAR) requests.

2.5 NON-COMPLIANCE AND ESCALATION

2.5.1 If an exception is found to be out of compliance with its compensating controls, a notification is sent to LOA Holder requesting remediation by a specific deadline.

2.5.2 Initial failure to remediate by the specified deadline will result in written notification to LOA Holder with a copy to their supervisor.

2.5.3 Secondary failure to remediate by the specified deadline will result in written notification to LOA Holder, their supervisor, and the appropriate Director.

2.5.4 Continued failure to remediate by the specified deadline may result in further escalation, including immediate revocation of approved exceptions.

REFERENCES:

Exception Process Method & Practice

CHAPTER 3

INFORMATION SECURITY MANAGEMENT

3.1 CYBERSECURITY INCIDENT REPORTING AND RESPONSE

All users of FDOT Information Technology are required to:

3.1.1 Report all suspicious activity to the FDOT Service Desk within 24 hours.

(a) This includes, but is not limited to, unlawful accesses, suspected system intrusions, theft, or other actions that may compromise the security of FDOT technology resources.

(b) An automated system is presented when contacting the FDOT Service Desk outside of normal operating hours, including weekends and holidays.

3.1.2 Provide all requested information, whether verbal or written, within the specified timeframe during investigations of suspected cybersecurity incidents.

3.1.3 Respond to final reports from FDOT Security Operations Center (SOC) investigation(s).

3.1.4 Establish any additional security controls that are deemed necessary by the SOC as a result of a cybersecurity incident investigation.

3.1.5 Follow all cybersecurity policies.

(a) Circumventing Department-configured security controls is prohibited and is considered a cybersecurity incident.

(b) Incidences of this will be reported to the appropriate Supervisor and/or Project Manager.

3.2 ELECTRONIC SECURITY FOR PUBLIC RECORDS EXEMPTIONS

This section applies to all electronic records created, stored, or processed through information systems within the Department.

3.2.1 All records of the Florida Department of Transportation are public records subject to disclosure, except those specifically made confidential or exempt by law.

3.2.2 Public records which are confidential or exempt are subject to special security considerations per appropriate Florida Statutes.

3.2.3 Electronic records which are exempt or confidential by law from the provisions of the *Public Records Law* shall not be released to any person without legal review by the Office of the General Counsel.

3.2.4 Owners of confidential or exempt electronic records are responsible for the security of that information. If the records are created, edited, stored, read, deleted, or transmitted electronically, the owner is responsible for the following:

(a) Ensuring any system with confidential or exempt data is documented in the Enterprise Change Management Database (CMDB) and flagged as confidential and exempt.

(b) Documenting and maintaining level of access of permitted persons within the Department's identity access management system.

(c) Ensuring that systems which include confidential or exempt data have a completed system security plan/system risk assessment.

(d) Ensuring that any processes which extract confidential electronic data from an original source still maintain the appropriate security for that data in transit and at rest.

3.3 SECURITY & USE OF CERTIFIED DIGITAL CERTIFICATES

This section establishes the minimum requirements and standards for acquiring, managing, and using Certified Digital Certificates within the Department's information technology infrastructure.

3.3.1 The authorized and legal notary may use an electronic signature to satisfy the notary requirement so long as all legally required information is attached to or logically associated with the signature or record.

3.3.2 The implementation of a Certified Digital Certificate (or "certificate") for specific processes requires Senior Management Service (SMS) or Traditional Select Exempt Service (SES) level approval.

3.3.3 The procurement of certified digital certificates shall be centralized and shall be processed through the Office of Information Technology (OIT).

3.3.4 Only approved FDOT and Other Personnel Services (OPS) employees are eligible for the installation and use of FDOT-procured Certified Digital Certificate vouchers (for new certificates) and/or order numbers (for renewals). Contractors are not eligible for FDOT-procured Certified Digital Certificates.

3.3.5 Department office units must create and submit a *Certified Digital Certificate Security Assessment* to Department's Information Security Manager (ISM) for review and approval prior to the implementation of certified digital certificates.

3.3.6 Users requiring a Certified Digital Certificate must request the certificate via the identity access management system.

3.3.7 Only the user to whom the Certified Digital Certificate is issued (Certified Digital Certificate Holder) may use the certificate.

3.3.8 Department purchased certified digital certificates shall only be installed on Department owned or leased information technology resources.

3.3.9 When a Certified Digital Certificate Holder no longer requires access to an assigned Certified Digital Certificate, the user's Supervisor or delegate must submit a request for removal via the identity access management system.

3.3.10 Digital certificates must be removed from all information technology resources within two business days of receiving separation notice or notice of a person no longer requiring the certificate.

3.3.11 Backing up and securing the Certified Digital Certificate is the responsibility of the Certified Digital Certificate Holder.

3.3.12 Misuse or abuse of certified digital certificates is subject to the Department's *Disciplinary Action Procedure, Topic No. 250-012-011,* and the *Disciplinary Standards* contained in *Rule 60L-36.005, F.A.C*.

REFERENCES:

Disciplinary Standards, Rule 60L-36.005, F.A.C.
Disciplinary Action Procedure*, Topic No. 250-012-011*
Methods & Practices (In development)

CHAPTER 4

ACCESS TO THE DEPARTMENT'S INFORMATION TECHNOLOGY RESOURCES

4.1 COMPUTER SECURITY PERSONNEL ROLES & RESPONSIBILITIES

The basic structure of security personnel is as follows:

4.1.1 The Information Security Manager (ISM) is responsible for ensuring the development, maintenance, and implementation of the Department's information security program.

4.1.2 The ISM is responsible for assisting in the development of security-related policies, procedures, and manual chapters; coordinating the Department information security risk management; and coordinating the Department's Cybersecurity Incident Response Team (CSIRT) and Security Operations Center (SOC).

4.1.3 The Transportation Support Director or delegate shall document and ensure the proper maintenance of access controls for Security Coordinators and Security Administrators managing information technology resources in each of their respective offices.

4.1.4 The FDOT Enterprise Security Team is responsible for documenting and maintaining statewide access selections for all of the Department's mainframe, network, and enterprise database infrastructures.

4.1.5 Cost Center Managers shall ensure that a separation request is submitted via the Department's identity management system no later than the user's separation date.

4.1.6 Security Coordinators will process all separation requests, notify application owners, and revoke access within two business days of the effective date or upon receipt of the request, whichever is later.

REFERENCES:

Security and Use of Information Technology Resources, *Topic No. 325-060-020*
Disciplinary Action Procedure*, Topic No. 250-012-011*
FLAIR Access Security, *Topic No. 350-090-150*
Section 282.318, Florida Statutes (F.S.)
Chapter 815, Florida Statutes (F.S.)
Rule Chapter 60GG-2, Florida Administrative Code (F.A.C.)
Rule Chapter 60L-36.005, Florida Administrative Code (F.A.C.)
Methods & Practices (In development)

CHAPTER 5

FIXED VOICE TELECOMMUNICATIONS EQUIPMENT

5.1 ADMINISTRATOR ACCESS

5.1.1 The Transportation Support Director or delegate shall designate the function of Network System Communications Administrator.

5.1.2 The Network System Communication Administrator shall be provided by the District to the CIO or delegate via email.

5.1.3 The Network System Communications Administrator operates in a position of trust and is responsible for granting Administrator access and granting and/or removing appropriate access on the telecommunications equipment via Local Administrative rights.

5.1.4 Access or removal of access must be requested through the identity access management system.

5.2 TELECOMMUNICATIONS EQUIPMENT ADMINISTRATOR TRAINING

5.2.1 The Administrators must complete training prior to being granted system access.

REFERENCES:

https://fldot.sharepoint.com/sites/FDOT-ECS/SitePages/Voice.aspx (for users)
Section 110.1082, F.S.
Methods & Practices (In development)

CHAPTER 6

USE OF CELL-ENABLED VOICE COMMUNICATIONS EQUIPMENT

6.1 PURCHASE & ACQUISITION OF CELL-ENABLED VOICE COMMUNICATIONS EQUIPMENT

6.1.1 Cell-enabled devices shall only be issued and used when cellular communications are required for job functions.

6.1.2 The purchase of cell-enabled devices for communications shall be approved by Cost Center Managers in accordance with the ***Commodities and Contractual Services Procurement Manual, Topic No. 375-040-020***.

6.1.3 The Cost Center Manager is responsible for authorizing the issuance of cell-enabled devices.

6.1.4 Individuals assigned state cell-enabled devices are required to report and pay for all personal usage, along with a service fee, pursuant to the instructions in the Department's Office of Comptroller's "***Disbursement Handbook for Employees and Managers***".

6.1.5 All staff assigned to manage cell-enabled communication accounts must have an approved identity access management system request for access to manage the cell-enabled communication accounts.

6.1.6 In accordance with ***Tangible Personal Property, Topic No. 350-090-310***, all cell-enabled devices are required to be recorded and updated. InTune data will be used for the maintenance and reporting of this requirement.

6.1.7 All Wireless Communication Account Managers must add Mobile Device Management staff to accounts as a maintain service plus role as designated by CIO or delegate.

6.1.8 New lines of service require SMS-level or above approval and the submission of an information resource request for approval.

6.2 CELL-ENABLED COMMUNICATION DEVICE SETUP

6.2.1 All cell-enabled devices must be enrolled in Apple Business Manager or Samsung Knox and location services must be enabled at the time the device is ordered and shipped to the business unit's Wireless Communications Account Manager.

6.2.2 The Wireless Communications Account Manager is responsible for enabling texting on the account by selecting the appropriate data plan when phones are ordered.

6.2.3 All staff assigned a Department-issued texting enabled device are responsible for ensuring the phones are in compliance with the Department's Text Messaging Policy, Topic No. 001-325-067.

6.2.4 After receipt of the cell-enabled device, the receiving Wireless Communications Account Manager must submit a service desk ticket for setup.

6.3 BILLING & PAYMENTS

6.3.1 All accounts must establish a process to authorize payment for monthly cellular service fees.

REFERENCES:

Commodities and Contractual Services Procurement Manual, *Topic No. 375-040-020*
Tangible Personal Property, *Topic No. 350-090-310*
Text Messaging Policy, *Topic No. 001-325-067*
Disbursement Handbook for Employees and Managers
Methods & Practices (In development)

CHAPTER 7

ACQUIRING TECHNOLOGY RESOURCES

7.1 INFORMATION RESOURCE REQUESTS

7.1.1 Information resource requests are required for the acquisition of all Information Technology Resources (ITRs) (including hardware, software, and data technology resources as defined in the *Enterprise Business Glossary*) with the following exceptions:

(a) Consumable supplies (paper, cables, printer toner, DVDs, etc.), or

(b) Computerized traffic systems and control devices which are used solely for the purpose of motor vehicle traffic control and monitoring.

7.1.2 Information Technology Service Managers (ITSMs) are responsible for conducting Service and Supportability Reviews prior to the acquisition of certain types of ITRs, as specified in Section 7.1.

7.1.3 All technology resources which are to be donated to the Department must have a completed and approved information resource request before the Department can accept such resources.

(a) Once donated to the Department, the original resource owner forfeits ownership of the resource.

7.2 TECHNOLOGY PURCHASING COST LIMITS

7.2.1 All technology purchases that have a total cost of $195,000 or more must be approved by the CIO and the Executive Director of Transportation Technology and reviewed with the Florida Digital Service.

REFERENCES:

Rule Chapter 60GG-5 (5), Florida Administrative Code (F.A.C.)
Methods & Practices (In development)

CHAPTER 8

TECHNOLOGY RESOURCE STANDARDS

8.1 DOCUMENTING TECHNOLOGY RESOURCE STANDARDS

8.1.1 The CIO or delegate is responsible for establishing and maintaining a list of technology resource standards for the Department.

8.1.2 The CIO or delegate is responsible for identification, evaluation, and approval of technology resource standards.

8.2 COORDINATING ADDITIONS OR CHANGES TO STANDARDS

8.2.1 Any requests for additions, deletions, or changes to standards must be submitted to and approved by the Technology Standards Review Team (TSRT).

8.2.2 Requests for exceptions to standards must be submitted and approved as outlined in Chapter 2, Exceptions.

8.3 ADOPTION OF STANDARDS

8.3.1 CIO or delegate is responsible for approving changes to Technology Resource Standards.

REFERENCES:

Section 282.0051(6), Florida Statutes (F.S.)
Section 216.181(5), Florida Statutes (F.S.)
Chapter 7 of this Manual (Acquiring Technology Resources)
Chapter 60GG-2, F.A.C.
Transportation Technology Standards Review Team (TSRT) Method &Practice

CHAPTER 9

ELECTRONIC DEVICE & MEDIA SANITIZATION

9.1 ELECTRONIC DEVICE & MEDIA SANITIZATION REQUIREMENTS

9.1.1 All electronic devices and media shall be sanitized prior to being disseminated within the Department, outside of the Department, or being disposed.

9.1.2 Each Cost Center Manager is responsible for ensuring the clearing and/or purging of confidential or exempt information prior to transfer, reuse, or disposal of hardware and electronic devices.

REFERENCES:

Media Sanitization Method & Practice
Support Services Manual

CHAPTER 10

REQUESTING SPECIAL SCHEDULING OF MAINFRAME RESOURCES

10.1 SCHEDULING MAINFRAME RESOURCES BEYOND REGULARLY SCHEDULED HOURS

10.1.1 Requests for scheduling outside of regular hours must be approved by CIO or delegate.

10.1.2 Requests for special scheduling of mainframe resources managed by third parties beyond regularly scheduled hours must be sent to the FDOT Service Desk no later than one (1) business day in advance.

REFERENCES:

Methods & Practices (In development)

CHAPTER 11

FDOT INTERNET REQUIREMENTS

11.1 INTERNET REQUIREMENTS

11.1.1 The Department's Website Content Management System (WCMS) must be used for the management of Internet and consultant websites.

11.1.2 All connections from the Department's internal network to the Internet must be made through the Department's firewall.

11.1.3 All web-enabled pages and sites must comply with the Americans with Disabilities Act and Section 508 of the Rehabilitation Act of 1973 and Section 60GG-2, F.A.C.

11.1.4 The purchase, ownership, renewal, and technical support of domain names must be initiated and managed by Central Office OIT.

REFERENCES:

Americans with Disabilities Act
Section 508 of the Rehabilitation Act of 1973
Chapters 119 and 815, Florida Statutes
Section 24(a), Article I, State Constitution
Security and Use of Information Technology Resources, *Topic No. 325-060-020*
OIT Standards for Web Domain Name Acquisition and Support
Methods & Practices (In development)

CHAPTER 12

FDOT INTRANET REQUIREMENTS

12.1 CONNECTING TO THE INTRANET

12.1.1 The CIO or delegate is responsible for determining the technology platform that will host the intranet.

12.2 DEVELOPING & PUBLISHING WEB PAGES, SHAREPOINT SITES, & APPLICATIONS ON THE INTRANET

12.2.1 All web-enabled pages and sites must comply with Americans with Disabilities Act and Section 508 of the Rehabilitation Act of 1973.

12.3 INTRANET DEVELOPMENT PROCESS

12.3.1 All websites, SharePoint sites, and applications published in the production environment must adhere to the Department's web development standards.

12.4 RESPONSIBILITY FOR INTRANET SITES, SHAREPOINT SITES, & WEB PAGES

12.4.1 The Cost Center Manager must ensure proper content and function of their respective offices' web sites, SharePoint pages, and application pages.

12.4.2 All Intranet sites must be registered with the Department's Webmaster.

REFERENCES:

Americans with Disabilities Act
Section 508 of the Rehabilitation Act of 1973
Section 282.206, Florida Statutes (F.S.)
Chapter 60GG-4, Florida Administrative Code (F.A.C.)
Static Web Standards
Web Application Standards
Chapter 8 of this Manual (Technology Resource Standards)
Employee Portal Link
Methods & Practices (In development)

CHAPTER 13

SOFTWARE LICENSE AGREEMENT

13.1 REQUIREMENTS FOR GRANTING A SOFTWARE LICENSE

13.1.1 The CIO or delegate must approve all legally binding license and code agreements.

13.1.2 Approval of CIO or delegate is required to enter into any third-party agreements related to software.

13.1.3 Software licenses purchased by the Department remain the property of the Department.

13.1.4 Software developed or outsourced by the Department remains the property of the Department.

13.1.5 Software license agreements between Florida State agencies must use Department form *Software License Agreement, Form No. 325-060-11*.

13.1.6 Software license agreements for non-Florida state agencies must use Department form *Software License Agreement, Form No. 325-060-12*.

REFERENCES:

Software License Agreement, Form No. 325-060-11 (for Florida State Agencies)
Software License Agreement, Form No. 325-060-12 (for Other State Agencies)
Methods & Practices (In development)

CHAPTER 14

ACCESS TO ANOTHER USER'S DATA

14.1 APPROVAL OF REQUESTS TO ACCESS OTHER USER'S DATA

14.1.1 Access to employee data requires documented electronic approval from the data owner.

14.1.2 If the data owner is unavailable to approve the request for access, that data owner's Supervisor can provide the approval.

(a) If the data owner is unavailable due to separation, their Supervisor can request this access via the identity access management system.

(b) The data owner's approved separation request within the identity access management system shall suffice as the required documented electronic approval.

(c) If data owner is unavailable for any other reason, their supervisor can request this access via email to their local IT Security Coordinator.

14.1.3 Once access is granted, notification is sent to the requesting Supervisor and Cost Center Manager.

14.1.4 Any request from Legal, OIG, or HR as part of an official investigation does not require additional approvals.

14.2 EXPIRATION OF ACCESS TO A SEPARATED USER'S DATA

14.2.1 Delegated access to a separated user's email box can be granted for thirty (30) days.

14.2.2 Delegated access to a separated user's email archive is perpetual until rescinded by Requestor.

14.2.3 Access to a separated user's OneDrive is granted to the Supervisor or delegate for a maximum of 180 days after the user account is deleted.

REFERENCES:

Methods & Practices (In development)

CHAPTER 15

EXTERNAL VPN ACCESS THROUGH THE DEPARTMENT OF MANAGEMENT SERVICES (DMS)

15.1 SECURITY COORDINATOR

15.1.1 The Transportation Support Director or delegate shall designate the function of Security Coordinators.

15.1.2 The Security Coordinators shall be provided by the District to the CIO or delegate via email.

15.1.3 The Security Coordinator operates in a position of trust and is responsible for provisioning access to IT asset.

15.2 REQUESTING VPN ACCESS

15.2.1 External partners that have a need to access Department data must have a request submitted on their behalf through the Department's identity access management system.

15.2.2 An authorized Department manager or delegate must request this access or removal of the access via the identity access management system.

15.3 ADMINISTRATOR ACCESS

15.3.1 The Cost Center making the request is responsible for maintaining the information within the necessary forms and documents.

15.3.2 The requesting Cost Center is responsible for ensuring that the external partner pays for the VPN service in a timely manner.

15.3.3 The requesting Cost Center is responsible for payment of any delinquent external partner accounts after 90 days.

15.3.4 The Security Coordinator is responsible for submitting the required Communications Service Authorization and Billing (CSAB) request for DMS VPN service or disconnect no later than 14 business days before the beginning of the next billing cycle.

15.3.5 It is the responsibility of each Transportation Support Director to cover any fees associated with the Security Coordinator not processing the timely cancellation of a VPN request.

REFERENCES:

282.702 F.S. and F.A.C.'s 60FF-1 – 60FF-6
Chapter 60GG-2, Florida Administrative Code (F.A.C.)
CSAB User Manual https://portal.suncom.myflorida.com/downloads/user_manual.pdf
Methods & Practices (In development)

CHAPTER 16

INSTALLATION & CHANGES FOR WAN CIRCUITS

16.1 SECURITY ADMINISTRATOR

16.1.1 The Transportation Support Director or delegate shall designate the function of Security Administrators.

16.1.2 Security Administrators in Communications Service Authorization and Billing System (CSAB) shall be provided by the District to the CIO or delegate via email. The CIO or delegate is responsible for providing Security Administrator information to DMS/Division of Telecommunications (DivTel).

16.1.3 Security Administrators operate in a position of trust and are authorized to make changes to existing circuits.

16.1.4 Security Administrators are responsible for maintaining an up-to-date inventory of circuit locations within their area of responsibility.

16.2 REQUESTING DATA CIRCUITS

16.2.1 Requests for data circuits must be submitted through the FDOT Service Desk.

16.2.2 Enterprise circuits are the responsibility of Central Office OIT.

16.3 CIRCUIT BILLING & PAYMENT

16.3.1 Central Office and Districts are responsible for direct billing and payment of their own services.

16.3.2 Each District Security Administrator is responsible for ensuring payments are processed.

16.4 CIRCUIT OPTIMIZATION & PURCHASING THRESHOLD

16.4.1 If consumption is consistently above 85% the impacted District should contact Central Office Integration Services to help address.

16.4.2 Each district is responsible for monitoring the bandwidth consumption on its circuits.

16.4.3 Director level or above approval is required for all circuit purchases or changes.

16.4.4 The Security Administrator is responsible for notifying CIO or delegate of any new, modified, or removed circuits within seven (7) days of Director-level or above approval.

16.5 EMERGENCY FAILOVER LOCATIONS

16.5.1 Upon request by Transportation Support Director or delegate, the Security Administrator must provide record of all office locations, including emergency failover locations, within their area of responsibility.

16.5.2 Each district must have two (2) designated failover locations.

16.5.3 CO and districts must be able to restore service at their regional headquarters to a minimum of 500 Mbps within one (1) hour.

REFERENCES:

Chapter 60GG-2.006(b), F.A.C.
CSAB User Manual https://portal.suncom.myflorida.com/downloads/user_manual.pdf
Methods & Practices (In development)

CHAPTER 17

APPLICATION DEVELOPMENT STANDARDS

These standards are required to be followed by any and all vendors, staff, or consultants employed by or contracted with FDOT. All information technology projects are reviewed against these standards for compliance.

17.1 APPLICATION DEVELOPMENT STANDARDS

17.1.1 All users of FDOT's information technology resources are required to comply with the OIT's Application Development Standards.

17.1.2 All projects that include customized code or data structures developed for FDOT are required to comply with these standards.

17.1.3 Commercial off the Shelf (COTS) products are required to adhere to these standards where applicable within the limits of the COTS product when custom development is being done on the product.

REFERENCES

Chapter 60GG-1, 60GG-2, and 60GG-5 F.A.C.
Application Development Standards
Methods & Practices (In development)