SECURITY ACCESS REQUEST FORM

USER INFORMATION

Name: _____ Existing/OIT User ID (if applicable): _____

E-mail Address: _____ Phone: _____

USER'S ACCEPTANCE OF CONDITIONS

By signing below, I signify that I have read and understand that I am subject to all the provisions of:

- **Chapter 119, Florida Statutes, Public Records**
- **Section 281.301, Florida Statutes – Safety and Security Services**
- **Chapter 282, Florida Statutes – Communications and Data Processing**
- **Section 282.318, Florida Statutes – Security of Data and Information Technology Resources**
- **Chapter 815, Florida Statutes – Computer Related Crimes**
- **Procedure 050-020-026 - Distribution of Exempt Documents Concerning Department Structures and Confidential and Exempt Security System**
- **Chapter 60GG-2, Information Technology Standards - Florida Administrative Code**

I understand that every employee is responsible for systems security to the degree that his or her job requires the use of information and associated systems. All users are responsible for using information resources only for the purposes for which they are intended, to comply with all controls established by information resource owners and custodians and for protecting sensitive information against unauthorized disclosure. I also understand that it is the user's responsibility to protect all of his or her passwords from being disclosed and to refuse to accept any other user's password.

I also understand that signing below indicates that I have read and completed the following:

FDOT Security's New Employee Required Reading:
http://www.dot.state.fl.us/computersecurity/ITPoliciesandStatutes.shtm
Computer Security Awareness for New Employees - Course and Quiz
http://www.dot.state.fl.us/computersecurity/SecurityAwarenessCourse.shtm

_____ _____
User's Signature Date

SAR TERMINATION REQUEST

☐ **Termination SAR**

Termination Submitted By:

_____ _____
Signature Date

REQUEST INFORMATION

Request Type: ☐ New User ☐ Name Change ☐ Access Change ☐ Termination

If termination is selected, please enter: Effective Date: _____ Effective Time: _____

New Account Type: *(Only for new accounts)* ☐ Employee/OPS ☐ Consultant/Contractor ☐ Generic/Service

Type of Computer Access Requested:

- ☐ Activu
- ☐ ESX/vSphere Admin
- ☐ Cyberkey *(Must complete Cyberkey Addendum)*
- ☐ FTP *(Must complete FTP Addendum)*
- ☐ Internet Access
- ☐ ITSFM *(Must complete ITSFM Addendum)*
- ☐ MIMS *(Must complete MIMS Addendum)*
- ☐ BlueTOAD
- ☐ iVEDDS *(Must complete iVEDDS Addendum)*
- ☐ SharePoint Online
- ☐ inSERVICE *(Road Ranger Only)*
- ☐ inSERVICE Manager *(Road Ranger Only)*
- ☐ SSL VPN *(Must complete SSL VPN Addendum)*
- ☐ PoC - Push-to-Talk *(Must complete PoC Addendum)*
- ☐ *E-Learning System (FLEX)*
- ☐ *Asset Tracking Portal (TRS)*
- ☐ *RTMC Phone System* *(Must complete Phone System Addendum)*

FOR FDOT APPROVAL

☐ IT Only – Technician – Justification: ☐

☐ IT Only – Domain Admin – Justification: ☐

☐ DOMAIN AND/OR LAN ACCESS – Specify Access: ☐

☐ FDOT SunGuide – Specify Access: ☐

☐ Operator	☐ Reporting	☐ Maintenance	☐ Read Only
☐ AAM	☐ Administrator	☐ Lead Operator	
☐ Supervisor	☐ Concessionaire	☐ Local Agency	

☐ CFX Sunguide **(By selecting this access, it does not give access to CFX Sunguide. This is for tracking purposes ONLY.)** ☐

REQUEST INFORMATION (Continued)

FOR FDOT APPROVAL

☐ ATSPM-Cloud – Specify Access:

- ☐ User
- ☐ Site Administrator

☐ BlueMac – Specify Access:

- ☐ Read Only
- ☐ Technician
- ☐ Lead Technician
- ☐ Engineer/Manager
- ☐ Administrator

☐ CMS – Specify Access:

- ☐ Read Only
- ☐ Location Management
- ☐ Administrator

☐ NOEMI – Specify Access:

- ☐ User
- ☐ Reporting
- ☐ Administrator

☐ R-ICMS – Specify Access:

- ☐ Viewer
- ☐ Agency User Response
- ☐ Response Plan Operator
- ☐ SOT Operator
- ☐ Operations Manager
- ☐ Corridor Manager
- ☐ Administrator

Select the Agencies Where Device Approval Authority is Needed:

- ☐ Daytona
- ☐ FDOT D5
- ☐ Lake County
- ☐ Maitland
- ☐ Marion County
- ☐ Melbourne
- ☐ Ocala
- ☐ Orange County
- ☐ Orlando
- ☐ Osceola County
- ☐ Palm Bay
- ☐ Palm Coast
- ☐ Seminole County
- ☐ Sumter County
- ☐ Titusville
- ☐ Volusia County
- ☐ Winter Park

☐ SELS – Specify Access:

- ☐ Reporting (Read Only)
- ☐ Operator
- ☐ Administrator

☐ MDP – Specify Access:

- ☐ User
- ☐ Manager
- ☐ Site Administrator

REQUEST INFORMATION (Continued)

FOR FDOT APPROVAL

☐ MMA – Specify Access:

☐ User

☐ SIIA – Specify Access:

☐ User ☐ Manager
☐ API ☐ Administrator

☐ Traffic Incident Management – Specify Access:

E-Learning System
☐ Publisher
☐ Administrator

Asset Tracking Portal
☐ Road Ranger Manager ☐ Administrator
☐ Device Checkout
☐ Asset Manager

☐ RTMC Phone System – Specify Access:

☐ System Admin ☐ Phone License Requested
☐ Manager Requested Group:
☐ Supervisor
☐ Operator

☐ Other – Specify Access:

MaxTime
☐ Read Only
☐ Editor

MaxView
☐ Read Only
☐ Editor

Solar Winds -- Select Agency --
☐ Read Only
☐ Administrator

InSync -- Select Agency --
☐ Read Only
☐ Administrator

MANAGERIAL APPROVAL

FDOT Supervisor's Name: Jeremy Dilmore

FDOT Supervisor's Signature: _____ Date: _____

Security Coordinator's Name: Steve Johnson

Security Coordinator's Signature: _____ Date: _____

FOR CONSULTANT/CONTRACTOR ACCESS ONLY

Project Manager's Name: _____ Phone: _____

Project Manager's E-mail Address: _____

Project Manager's Signature: _____ Date: _____

Consultant Company Name: _____

Project Number/Description: _____

Project Start Date: _____ Project End Date: _____

Consultant Representative's Name: _____ Phone: _____

Consultant Representative's Title: _____

ADDITIONAL COMMENTS

Florida Department of Transportation
719 South Woodland Boulevard
Deland, FL 32720

RON DESANTIS
GOVERNOR

JARED W. PERDUE, P.E.
SECRETARY

Please attach completed form to a Facility Work Order or e-mail to D5-Facilities-All@dot.state.fl.us for *badge issuance and activation*. If you have any questions, please call (386) 943-5011.

General Information:

Name: _____ Company/Firm: _____

Consultant, Contractor, or Vendor: _____ External Consultant: ☐ YES ☐ NO

Start Date: _____ Contact Phone Number: _____

Access Information:

FDOT Access Requestor: _____ Department/Cost Center: TRAFFIC OPERATIONS

Access Points Requested:

Basic Mon- Fri 6 AM- 6 PM: _____ Basic Extended Mon-Sun 6 AM-6 PM: _____ Extended Mon-Sun 24/7: _____

Holiday Access: _____ Data/Radio Comm Rooms: _____ Crew Building: _____ Warehouse: _____

Additional Access Required? _____

RTMC Access Information:

Agency |FDOT: ☐ FWC: ☐ FHP: ☐

Manager ☐ Supervisor: ☐ Operator: ☐ Employee: ☐ Consultant: ☐ OIT: ☐

Additional Access Required: ☐ _____

By accepting this badge, I agree to immediately notify Facilities Management if the badge is lost or stolen.

_____ _____
Consultant/Contractor Signature **Date**

Approved by Cost Center Manager or Above:

_____ _____
Signature **Date**

Facilities Use Only

Processed by: _____ Badge Number: _____

Date: _____

Cyberkey Access Request Addendum

REQUEST INFORMATION

Name: _____ User ID (if known): _____

Company: _____ Phone: _____

Address: _____

City: _____ State: _____ Zip: _____

E-mail Address: _____

Scope of Work

Duration of Work

Start/Active Date: _____ End/Expiration Date: _____

USER'S ACCEPTANCE OF CONDITIONS

By signing below, I agree with the following:

- I understand that this cyberkey is for the use of the requestor **ONLY**. The cyberkey is **NOT** allowed to be shared.
- I understand that I am required either have the cyberkey on my person or in a **SECURE** location when not in use.
- Failure to lock a location when leaving could result in the termination of cyberkey access.
- Failure to charge/authorize at least once a month or access a location at least once every six months with your assigned cyberkey will result in the termination of cyberkey access and must be returned.
- If lost, stolen or damaged, the requestor is responsible for the replacement of the cyberkey at their cost.
- If lost or stolen, the requestor is required to notify D5 TSM&O Security via e-mail (D5.TSMOSecurity@dot.state.fl.us) **IMMEDIATELY**.
- The cyberkey is required to be returned by 4:00PM on the business day following the End/Expiration Date, if set.

_____ _____

User's Signature Date

FDOT USE ONLY

Cyberkey ID: _____

D5 TSM&O EXTERNAL FTP Access Request Addendum

Employee/Consultant Name: _____
(print name)

User ID (if known): _____

Phone Number: _____

Consultant's E-mail Address: _____

Consulting Firm Name: _____

Indicate directory structure or path where you will place your files. _____

The directory will be created for you. All directories are created after the following path: "ftp://ftp.cflsmartroads.com/external/"

*** Important information concerning the external FTP Server ***

- The external FTP server does not allow anonymous access. If you require access, this completed form is required.
- FTP user accounts will only receive write and delete access to only the requested folder(s). All other folders will be read only except for folder contained
- FTP user accounts are locked out after 3 unsuccessful login attempts.
- Passwords must be changed every 65 days. Failure to do so will lock your account. Change the FTP user account password at the following site:
- You will not receive any warnings prior to the time of the expiration of your FTP user account password, so please use some calendar/alarm to remind you to change your FTP user account password.
- Files older than 14 days are automatically deleted within the external folder.
- Accounts that remain inactive for 365 days are deleted from the server.
- Any and all files placed on the FTP server are subject to review by D5 TSM&O Security. The use of the external FTP server for any activity other than FDOT business is strictly prohibited.
- Sharing usernames and passwords is prohibited.
- Any and all problems should be reported to D5 TSM&O Security via e-mail at D5.TSMOSecurity@dot.state.fl.us.

I have read the above information and agree: _____
Employee/Consultant Signature

FDOT TSM&O Supervisor/Project Manager (Print) - Authorization	Signature	Date

Jeremy Dilmore		
FDOT TSM&O Security Administrator (Print) - Authorization	Signature	Date

ITSFM Access Request Addendum

What is ITSFM? The ITS Facility Management System (ITSFM) provides users the ability to manage and document District 5's fiber, power, and inventory information.

What are the differences in roles? ITSFM is divided into three user roles ranging from a standard view access to full access to all features within a Serving Area. The roles are:

- **System Manager** – This User has the ability to generate custom management reports including user and equipment site active reports
- **Editor** – This User has full rights to add, modify and delete data. The Users assigned this role are limited in number and only assigned to the most experience Users. Editors can add or modify fiber connectivity and any errors would result in serious problems for the system.
- **Maintainer** – This User has limited rights to edit information existing in the database. This role is assigned to Users such as a Maintenance Technician who need the ability to updated attributes resulting from equipment replacements but do not need full Editor Rights. This User cannot place new features, or delete existing features; they can only edit attributes for the existing feature. This User is not allowed to make any changes that effect fiber connectivity such as changing fiber jumper assignments or fiber status.
- **Viewer** – This User can view data, perform locates, spatial queries and run reports, but cannot add, modify or delete features or data. This role is assigned to Users who only need the ability view information and generate reports.

AUTHORIZED AGENT INFORMATION

Name: Jeremy Dilmore Phone: 386-943-5360

E-mail Address: Jeremy.Dilmore@dot.state.fl.us

I request the FDOT Central Office ITS Section grant access of my agency's transportation management facility managed within the ITSFM system to the person listed below. This person is authorized to access the following Serving Area(s) and shall be assigned to the User Role shown below to support the maintenance of our database information stored in the ITSFM. Furthermore, I also verified that this individual has passed a Florida Department of Law Enforcement (FDLE) or State Law Enforcement Radio System (SLERS) background check.

Signature: _____ Date: _____

ITSFM USER INFORMATION

First Name: _____ MI: _____ Last Name: _____ Phone: _____

E-mail Address: _____

Company: _____ Title: _____

Department: _____

Address: _____ City: _____ State: _____ Zip: _____

SERVING AREA AND USER ROLE

Serving Area	*User Role*	*Action*
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --

ITSFM Access Request Addendum

SERVING AREA AND USER ROLE (Continued)

Serving Area	*User Role*	*Action*
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --
-- Select Area --	-- Select Role --	-- Select Action --

MIMS Access Request Addendum

What is MIMS? The Maintenance and Inventory Management System (MIMS) provides users the ability to create and manage trouble tickets, maintenance activities and asset inventory.

Who uses this form? Florida Department of Transportation District Five currently requires MIMS for its maintenance contractors for the purpose of maintenance operations and asset management. It is restricted in use and requires access to the D5 TSM&O Network either via direct connection or VPN access. Please use the form below to request a user ID and password for the application. One form needs to be completed for each person in your organization that will use the application.

USER INFORMATION

Name: _____ Phone: _____ Fax: _____

Title: _____ Agency: _____

E-mail Address: _____

Address: _____ City: _____ State: _____ Zip: _____

REQUESTED ACCESS

☐ MIMS Administrator – Justification:

Contract Group Access:

☐ D5 RTMC – Specify Access: -- Select Access --

☐ D5 ACS – Specify Access: -- Select Access --

☐ D5 ITS – Specify Access: -- Select Access --

☐ D5 Construction – Specify Job(s) and Access:

☐ D5 Transcore – Specify Access: -- Select Access --

☐ City of Orlando – Specify Access: -- Select Access --

☐ Osceola County – Specify Access: -- Select Access --

I understand that access to this system requires direct access to the D5 TSM&O Network either via a direct connection or VPN access. This system cannot be access through the internet.

I also understand that if assistance is needed the MIMS user is responsible for contacting D5 TSM&O Security via e-mail at D5.TSMOSecurity@dot.state.fl.us.

_____ _____

User's Signature Date

Inter-agency Video and Event Data Distribution System (iVEDDS)
Access Request Addendum

What is iVEDDS? The Inter-agency Video and Event Data Distribution System (iVEDDS) distributes live motion CCTV camera video feeds from FDOT District Five utilizing the internet. This tool provides streaming video from CCTV locations along I-75, I-95, and I-4. Also offered in this application is event data, which provides a full list of traffic events and is hyperlinked to detail screens that provide time stamps, chronology, emergency responders, and other incident clearance information. The event data runs off of the SunGuide traffic incident management database, which powers real-time updates.

Who uses this form? Florida Department of Transportation District Five currently offers iVEDDS to first responders and public agencies for no charge. However, it is restricted in use and not available to the general public or private entities due to bandwidth capacity. Please use the form below to request a user ID and password for the application. One form needs to be completed for each person in your organization that will use the application.

What access does this form provide? This form provides access to the video and/or event data contained in the iVEDDS application. This **does not** provide access to the District Five TSM&O network.

USER INFORMATION

Name: _____ Phone: _____ Fax: _____

Title: _____ Agency: _____

E-mail Address: _____

Address: _____ City: _____ State: _____ Zip: _____

USER'S ACCEPTANCE OF CONDITIONS

By signing below, I signify that I have read and understand that I am subject to all the provisions of:

- **Executive Office of the Governor Memorandum – 1998-01, Information Resource Security Policy**
- **Chapter 119, Florida Statutes, Public Records**
- **Section 281.301, Florida Statutes – Safety and Security Services**
- **Chapter 282, Florida Statutes – Communications and Data Processing**
- **Section 282.318, Florida Statutes – Security of Data and Information Technology Resources**
- **Chapter 815, Florida Statutes – Computer Related Crimes**
- **Procedure 050-020-026 – Distribution of Exempt Public Documents Concerning Department Structures and Security System Plans**
- **Chapter 60GG-2, Information Technology Standards - Florida Administrative Code**

- It is the user's responsibility to protect all passwords from being disclosed and to refuse to accept any other user's password. Sharing usernames and passwords is strictly prohibited.
- Accounts that remain inactive for 180 days are deleted from the system.
- I understand that if assistance is needed with using this system the iVEDDS user is responsible for contacting D5 TSM&O Security via e-mail at D5.TSMOSecurity@dot.state.fl.us

_____ _____

User's Signature Date

SSL VPN Access Request Addendum

Customer Information:

User ID (if known): _____

Name: _____

Company Name: _____

Street Address: _____

City: _____

State/Zip Code: _____

Phone Number: _____

Technical Contact Information:

Contact Name: _____

Contact Phone No.: _____

Contact E-mail Address: _____

I understand the FDOT does not allow split tunneling for VPN access. This means that during a VPN session with FDOT, I will not have direct access to my local area network.

I also understand that if technical assistance is needed the VPN user is responsible for contacting D5 TSM&O Security via e-mail at D5.TSMOSecurity@dot.state.fl.us.

Print Name	Signature	Date

District Five Push-to-Talk over Cellular (PoC)
Access Request Addendum

What is District Five's PoC System? Push-to-Talk over Cellular (PoC) provides two-way radio services over Long Term Evolution (LTE) technology, creating a radio network that utilizes the cellular infrastructure of Mobile Network Operators. It is the primary source of direct push-to-talk communication to the Regional Traffic Management Center.

Who uses this form? Florida Department of Transportation District Five utilizes a Push-to-Talk over Cellular (PoC) system for direct communication to the Regional Traffic Management Center operators. The system is authorized to contractors, FDOT staff, and emergency responders for the purpose of traffic incident management communication, asset management, and event management. It is restricted in use and requires such users to have authorization and clearance. Approved authorization includes:

- State Law Enforcement Radio System (SLERS) background
- A letter of authorization from a Chief or Sheriff of a government entity that provides either law enforcement or fire/EMS services.
- A letter of authorization from District Five's Traffic Operations Engineer, Director of Transportation Operations, or their designee.

Please use the form below to request access to the Florida Department of Transportation District Five Push-to-Talk over Cellular (PoC) system.

USER INFORMATION

Name: _____ Phone: _____

Title: _____ Agency Name: _____

Agency Address: _____ City: _____

State: _____ Zip Code: _____ Agency Phone Number: _____

Email Address: _____

Agency Type: Road Ranger Authorized By: SLERS Background

REQUESTED TYPE

Access Type: System User

Requested Zone: ☐ CFX ☐ Interstate 4 ☐ Interstate 95 ☐ Interstate 75 ☐ Other: _____

PoC USER'S ACCEPTANCE OF CONDITIONS

By signing below, I signify that I have read and understand that I am subject to all the provisions of:

- Executive Office of the Governor Memorandum – 1998-01, Information Resource Security Policy
- Chapter 119, Florida Statutes, Public Records
- Section 281.301, Florida Statutes – Safety and Security Services
- Chapter 282, Florida Statutes – Communications and Data Processing
- Section 282.318, Florida Statutes – Security of Data and Information Technology Resources
- Chapter 815, Florida Statutes – Computer Related Crimes
- Chapter 60GG-2, Information Technology Standards - Florida Administrative Code
- Procedure 050-020-026 – Distribution of Exempt Public Documents Concerning Department Structures and Security System Plans
- Department of Management Services Joint Task Force on State Agency Law Enforcement Communications Standard Operating Procedures (SOP's) regarding the State Law Enforcement Radio System (SLERS).
- Chapter 60GG-2, Information Technology Standards - Florida Administrative Code
- **It is the user's responsibility to protect all passwords and tokens from being disclosed and to refuse to accept any other user's password. Sharing usernames and passwords as well as device tokens is strictly prohibited. You agree to immediately notify us of any unauthorized use of your password or account or any other breach of security.**
- **It is the user's responsibility to report any system security concerns or when a device that has access to the PoC system is lost or stolen imminently and without delay via the Jira Reporting System (jira@fdotd5.atlassian.net).**
- **I understand that if assistance is needed with using the PoC System the user is responsible for contacting D5 TSM&O via the Jira Reporting System (jira@fdotd5.atlassian.net).**
- **You agree that FDOT, in our sole discretion, may suspend or terminate your account (or any part thereof), for any reason, including, without limitation, if we have reason to believe that you have violated any rules or provisions of this system. Any suspected fraudulent, abusive, or illegal activity will be grounds for termination of your account and services provided. Any fraudulent, abusive, or illegal activity may be referred to appropriate law enforcement authorities.**

_____ _____

User's Signature Date