

Approved:

Effective: May 18, 2010
Review: July 12, 2019
Office: Right of Way
Topic No.: 575-095-010-c



Department of Transportation

RIGHT OF WAY MANAGEMENT SYSTEM SECURITY

AUTHORITY:

Sections 20.23(4)(a) and 334.048(3), Florida Statutes

REFERENCES:

RWMS User Manual, Chapter 12, People Management

STATEMENT OF POLICY:

To define the process to follow to grant or remove the authorization of a user to create, update, and delete records in the Right of Way Management System (RWMS).

SCOPE:

District and Central Offices of Right of Way will utilize this procedure.

DEFINITIONS:

District Security Coordinator: The District position responsible for the creation and management of RWMS security profiles within the district. In addition, the RWMS District Security Coordinator will maintain documentation detailing the approval, creation, and removal of all security profiles within the district.

RWMS (Right of Way Management System): A web-based computer application that is the primary computer application used by the Office of Right of Way.

Security Administrator: The Central Office position responsible for granting and removing RWMS District Security Coordinator security profiles. In addition, this position will coordinate all RWMS security related issues with the RWMS District Security Coordinators. The RWMS Security Administrator will periodically review District

compliance with this procedure. There will be one RWMS Security Administrator and one backup assigned in the Office of Right of Way in the Central Office.

Security Profile: A defined list of authorities that allows a user to create, update, and delete records in one or more areas of RWMS.

GENERAL

Any employee or consultant that has been assigned a valid FDOT UserID and access to the FDOT Infonet can log into RWMS as a read-only user. The ability to create, update, and delete data in RWMS must be strictly controlled and any user that requires this authorization in RWMS must submit a request and have the request approved by the appropriate manager or delegate as described in this procedure.

1. PROCESS FOR RWMS SECURITY

1.1 ASSIGNMENT OF RWMS SECURITY ADMINISTRATOR

- 1.1.1** Prior to the implementation of RWMS, the Central Office assigned one user as the RWMS Security Administrator and at least one user as a backup.
- 1.1.2** If Central Office needs to change who is assigned as the RWMS Security Administrator or backup for any reason, the Director, Office of Right of Way, will notify the District Right of Way Managers and the RWMS District Security Coordinators (written or e-mail) of the change.

1.2 ASSIGNMENT OF RWMS DISTRICT SECURITY COORDINATORS

- 1.2.1** Each District will assign one user as the RWMS District Security Coordinator for their District and at least one user as a backup for their District. The names and UserID's of the RWMS District Security Coordinators will be submitted to the RWMS Security Administrator in Central Office.
- 1.2.2** If a District needs to change who is assigned as the RWMS District Security Coordinator or backup for any reason, the District Right of Way Manager shall submit a request (written or e-mail) to the RWMS Security Administrator that includes the name and UserID of the new RWMS District Security Coordinator and the name and UserID of the RWMS District Security Coordinator that will be replaced. In addition, the request will include an effective time and date for the change. The RWMS Security Administrator will notify the District Right of Way Manager upon completion of the request.

1.3 REQUESTING AUTHORITY TO CREATE, MODIFY, AND DELETE RECORDS IN RWMS

- 1.3.1** A user must acquire or possess a valid FDOT UserID. The Office of Information Systems has established procedures for requesting UserID's for new employees and consultants.
- 1.3.2** The District Right of Way Manager can delegate the authority to approve or reject requests submitted under **Section 1.3.3** to any District Right of Way employee with the exception of the District RWMS Security Coordinator. The District Right of Way Manager will notify (written or e-mail) the District Right of Way employee receiving the delegated authority, RWMS District Security Coordinator, and the RWMS Security Administrator.
- 1.3.3** The employee or consultant's immediate supervisor or a higher-level supervisor shall submit a request (written or e-mail) to the District Right of Way Manager or delegate requesting authority for the employee or consultant to create, modify, and delete data in RWMS. The request shall include the employee or consultant's name, UserID, security profile types that are to be assigned to the employee or consultant, and an effective date and time, if different than the date of the request. For a description of each security profile type, see the ***RWMS User Manual, Chapter 12, People Management***.
- 1.3.4** The District Right of Way Manager or delegate will either approve or reject the request. If approved, written requests shall be signed and sent to the RWMS District Security Coordinator for completion. If the request was made via e-mail, the District Right of Way Manager or delegate shall forward the e-mail with their approval to the RWMS District Security Coordinator for completion.
- 1.3.5** The RWMS District Security Coordinator will complete the request within two working days of the effective time and date contained in the request and notify the user and supervisor that the request was completed.
- 1.3.6** The RWMS District Security Coordinator will not add or modify any security profiles without prior approval of the District Right of Way Manager or delegate.

1.4 REMOVING AUTHORITY TO CREATE, MODIFY AND DELETE RECORDS IN RWMS

- 1.4.1** The District Right of Way Manager can delegate the authority to approve or reject requests submitted under **Section 1.4.2** to any District Right of Way employee with the exception of the District RWMS Security Coordinator. The District Right of Way Manager will notify (written or e-mail) the District Right of Way employee receiving

the delegated authority, RWMS District Security Coordinator, and RWMS Security Administrator.

- 1.4.2 If an employee or consultant's authority to create, modify, and delete records in RWMS needs to be removed for any reason, the employee or consultant's immediate supervisor or a higher-level supervisor shall submit a request (written or e-mail) to the District Right of Way Manager or delegate for the removal of the employee or consultant's authority to create, modify, and delete data in RWMS. The request shall include the employee or consultant's name, UserID, security profile types that are to be removed, and the effective date and time, if different than the date of the request that the removal needs to occur on. For a description of each security profile type, see the ***RWMS User Manual, Chapter 12, People Management***.
- 1.4.3 The District Right of Way Manager or delegate will either approve or reject the request. If approved, written requests shall be signed and sent to the RWMS District Security Coordinator for completion. If the request was made via e-mail, the District Right of Way Manager or delegate shall forward the e-mail with their approval to the RWMS District Security Coordinator for completion.
- 1.4.4 The RWMS District Security Coordinator will complete the removal request within one working day from the effective time and date contained in the request and notify the supervisor that the request was completed.
- 1.4.5 The RWMS District Security Coordinator will not remove any security profiles without prior approval of the District Right of Way Manager or delegate.

2. DOCUMENTATION

- 2.1 RWMS District Security Coordinators are responsible for maintaining documentation of all requests to add or remove security profiles in RWMS. The documentation may be in hard copy or electronic format. .
- 2.2 The RWMS Security Administrator is responsible for maintaining documentation of all requests to add or remove RWMS District Security Coordinator security profiles. The documentation may be in hard copy or electronic format.

3. TRAINING

No formal training is required.

4. FORMS

No forms are required by this procedure.