Approved:

Effective: June 14, 2017
Review: April 21, 2017
Office: Comptroller
Topic Number: 350-090-150-j

Department of Transportation

FLAIR ACCESS SECURITY

PURPOSE:

This procedure defines requirements for, and removal of, access to FLAIR information to minimize inadvertent employee error and negligence and reduce opportunities for computer related crime. It also addresses the custodial responsibilities as required by Florida Department of Financial Services.

AUTHORITY:

Section 20.023(3)(a) and 334.048(3), Florida Statutes

REFERENCES:

FLAIR Procedures Manual, Department of Financial Services
Chapter 2, Information Technology Resource User's Manual, Topic No. 325-000-002
Procedure No. 350-030-010, Purchasing Card
Department of State, Records Retention Schedule, GS1-SL V
Section 282.318, Florida Statutes (F.S.)
Section 215.93, Florida Statutes (F.S.)
Chapter 815, Florida Statutes, Computer Related Crimes

SCOPE:

The principal users of this document will be those that are required by their position or duties to monitor, access, or process Department financial transactions through FLAIR and their supervisors that are authorizing access.

DEFINITIONS:

AARF: Automated Access Request Form. This system is used to request or terminate FLAIR access.

Access Control Custodian: The individual(s) designated by each agency responsible for establishing and terminating user access within the FLAIR Access Control File.

District Purchasing Card Administrator: The individual in each district (including Central Office) authorized to maintain FLAIR access control for the CD function (Purchase Card) only. The list of administrators is located at https://fldot.sharepoint.com/sites/FDOT-OOC/DOO/PCard/Lists/PCard%20Administrators/AllItems.aspx.

FTA: File Transfer Appliance. This system is a secure and encrypted method of electronically transferring files.

FLAIR: Florida's Accounting Information Resource.

FLAIR User Agreement: A required agreement to be completed and signed by each user prior to obtaining access to FLAIR. The form is available at link on OOC Sharepoint site: https://fldot.sharepoint.com/sites/FDOT-OOC/SitePages/Home.aspx

OOC: Department of Transportation, Office of Comptroller.

OOC FLAIR Security Team: The team members responsible for granting and terminating FLAIR access for all Department of Transportation employees needing such access (also referred to as Access Control Custodians). This team operates the FDOT-FLAIR Security mailbox (FDOT-FLAIRSecurity@dot.state.fl.us).

Purchasing Card Program Administrator: Coordinates, monitors, and oversees the Purchasing Card Program, and ensures that key controls are in place and operate as designed.

1. SECURITY REQUIREMENTS

Section 282.318, F.S., Security of Data and Information Technology Resources, establishes security requirements for all state agencies. The willful and knowing unauthorized use, alteration or destruction of information assets is a computer-related crime punishable under the provisions of ***Chapter 815, F. S., Computer Related Crimes***.

2. REQUESTING FLAIR ACCESS

2.1 Supervisors will be responsible for determining FLAIR access requirements for their respective employees.

2.2 The employee will be required to complete and sign a FLAIR User Agreement

2.3 The supervisor will submit an AARF request for the appropriate FLAIR access. The FLAIR User Agreement must be scanned/uploaded using the AARF addendum. AARF will route the request through the multiple approvals required prior to granting FLAIR access. After all approvals have been received, FLAIR access will be established and a secured email containing the username and temporary password will be sent to the employee.

2.4 To ensure proper segregation of duties, the Purchasing Card Administrator(s) may not be granted the Access Control Custodian role in FLAIR.

3. RESTORING PASSWORDS

3.1 If the timeframe for a FLAIR username has expired and the system will not allow access, the employee must submit a request via email to the OOC FLAIR Security Team to request a password reset. The email must include the username for which the password is to be reset. Only the owner of the username may request a password reset.

3.2 The OOC FLAIR Security Team will notify the employee by secured email when the password is reset.

4. CHANGING ACCESS OR DELETING USER NAMES

4.1 When an employee transfers to another position within the Department or terminates from the Department, the respective supervisor (or their designee) must notify the OOC FLAIR Security Team by submitting an AARF request indicating the user access is to be changed or terminated. This request must be submitted on or before the effective date of transfer or termination.

4.2 As soon as notification is received, the OOC FLAIR Security Team will change or terminate access as requested.

5. CD FUNCTION ONLY (Purchasing Card Function)

Users may request access to the CD function through the AARF process as specified in Section 2.2. Once the AARF request is approved and finalized, the OOC FLAIR Security Team is responsible for notifying the appropriate District Purchasing Card Administrator and Purchasing Card Program Administrator with the confirmation of the username and FLAIR access. When this notification is received, the District Purchasing Card Administrator is responsible for granting the user the appropriate access within the FLAIR

purchasing card module. Only authorized employees will be granted access in accordance with procedure 350-030-010, Purchasing Card.

6. RECORD RETENTION

All FLAIR access requests will be retained by the AARF system. All correspondences through the OOC FLAIR Security Team inbox will be retained in accordance with the Florida Department of State Records Retention Schedule.

7. MONITORING

7.1 The OOC FLAIR Security Team will monitor the ***PPS Termination Report*** weekly to identify and terminate FLAIR access for former employees, even if an AARF request has not been submitted. If an AARF termination request has not been submitted, an email will be sent to the supervisor's manager to advise them of the requirement defined in ***section 4.1***.

7.2 A FLAIR ***Access Control Report*** may be viewed on the following SharePoint site for the Office of Comptroller:

https://fldot.sharepoint.com/sites/FDOT-OOC/SitePages/Home.aspx

All Financial Services Managers in the Districts and Office of Comptroller must review this report monthly. If a change is needed based on this review, an AARF request must be submitted immediately (see ***section 4***).

8. TRAINING

The Performance Management Office offers Computer Security Awareness training online (CU-11-0613) located at:
http://infonet.dot.state.fl.us/bsso/RTS/services/cbt/courses.htm.

Florida Depart of Financial Services provides a FLAIR Procedures Manual located at:
http://www.myfloridacfo.com/Division/AA/Manuals/100FLAIRFundamentals.pdf