CHAPTER 2

ACCESS TO THE DEPARTMENT'S INFORMATION TECHNOLOGY RESOURCES

PURPOSE:

To define the requirements for obtaining and removing access to the Florida Department of Transportation's (Department or FDOT) information technology (IT) resources.

AUTHORITY:

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

SCOPE:

This procedure applies to any member of the Department's workforce using the Department's information technology resources. The Department's information technology resources include, but are not limited to, the mainframe and its applications and associated data, network applications and associated data, cloud applications and associated data, networks, e-mail, Internet, Intranet, file transfer services, and remote access services.

Districts must implement procedures or processes that meet or exceed the Department requirements in this procedure.

REFERENCES:

Security and Use of Information Technology Resources, Topic No. 325-060-020
FLAIR Access Security, Topic No. 350-090-150
Rule Chapter 60L-3536.005, Florida Administrative Code (FAC)
Rule Chapter 60GG-2, Florida Administrative Code (FAC)
Topic No. 250-012-011, Disciplinary Action
Chapter 815, Florida Statutes (F.S.)
~~Chapter 74-2, Florida Administrative Code (F.A.C.)~~
Section 282.318, Florida Statutes (F.S.)

Formatted: Indent: Left: 0", First line: 0"

BACKGROUND:

Per Section 815.06, F.S., whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

2.1 COMPUTER SECURITY PERSONNEL ROLES AND RESPONSIBILITIES

The **Department** is a decentralized organization and has established a decentralized network of **personnel** who perform **computer security** tasks. These personnel are the primary contacts for obtaining **access** to computer network resources.

2.1.1 The basic structure of security personnel is as follows:

(1) The Information Security Manager (ISM) is responsible for ensuring the development, maintenance, and implementation of the Department's information security program. Additionally, the ISM is responsible for assisting in the development of security--related policies, procedures, and manual chapters, coordinating Department information security risk management, and coordinating the Department's Computer Security Incident Response Team. The Department's Secretary is responsible for the annual appointment of the ISM.

(2) The District IT Services Manager is responsible and accountable for ensuring the proper maintenance of access controls for **information technology resources** in each of their respective offices.

(3) The **FDOT Enterprise Security Team** is responsible for documenting and maintaining statewide access controls for all the Department's mainframe, network, and enterprise database infrastructures. The FDOT Enterprise Security Team shall maintain a list of Business Coordinators and Office of Information Technology (OIT) Security Coordinators by name and function

on the ~~FDOT Security webpage~~FDOT Security webpage and on the FDOT Employee Portal.

Formatted: Default Paragraph Font

(4) **OIT Security Coordinators** are responsible for OIT security tasks to maintain access controls for information resources, applications, or environments. Examples of OIT Security Coordinator duties include user provisioning, client application support, desktop security support, and FDOT Enterprise Security Team. In some cases, one individual (such as a District IT Services Manager) may be responsible for several OIT security coordinator functions. The following ~~individuals~~ roles support the Department's OIT Security Infrastructure:

(A) ~~**Functional Application**~~**F**unctional Application Owners are responsible for approving and maintaining access controls for a particular application. ~~-~~Examples include the person who authorizes access controls for the Financial Management System (FM) or the Right-of-Way Management System (RWMS). The **application owner** must designate the functional application owner.

(B) **Physical Access Coordinators** are individuals responsible for computer-controlled physical access systems, such as card swipe access systems.

(C) **Access Coordinators** are responsible for granting access to an information resource, application, or environment. The Functional Application Owners and/or Access Coordinators are responsible for confirming the need for access, the need for the requested access level, and granting or denying the access. Access coordinators grant access and acknowledge in the ***Automated Access Request Form (AARF) System*** ~~AARF~~ when approval is received from the Functional Application Owner. In some cases, the Functional Application Owner can also serve as the Access Coordinator.

(D) **Business Coordinators** are responsible for the IT Security needs in their cost center. They do not have RACF/AD Security to grant access. An example is ~~Examples include~~ the person who assists the new employees in completing ~~the needed~~ security forms and by providing ~~them with~~ the "new-user" login~~on~~ credentials to read security-related policies, procedures, statutes. SES and SMS managers are responsible for notifying the FDOT Enterprise Security

Team in writing (hard-copy or e-mail) when the Business Coordinator is selected or changed.

(E) Application Security Coordinators are responsible for granting access to RACF security groups within their application.

(F) ISA (Internet Subscriber Account) Application Administrators are responsible for Maintaining ISA user access to their application by activating or inactivating ISA users as necessary. ISA Application Administrators support their application's ISA users with login-related issues and reset ISA passwords for their application users.

~~(F)~~

Formatted: No bullets or numbering

2.2 Access Controls for User-IDs

2.2.1 All authorized users of the Department's computer network resources must:

(1) Be requested via the AARF system.

(2) Have a unique user identification (user-ID).

(3) Have a complex password that authenticates~~identifies~~ them to the information technology resource.

RACF serves as the Department's official repository for user-IDs. Exceptions to the following user-ID requirements shall be reviewed and approved or disapproved on a case-by-case basis by the Department's ISM and shall be requested and documented within the AARF System. To the extent possible, the same user-ID shall be used for accessing all information technology resources.

2.2.2 Standard User-IDs: Standard user-IDs are assigned to specific individuals and are used exclusively by that individual for access to computer network resources. Standard user-IDs shall use the following naming conventions:

(1) User-IDs shall consist of seven (7) characters (alphanumeric).

(2) The first two (2) characters (alpha) are the identification of the user's organizational unit.

(3) The next three (3) characters (numeric) are the cost center of the user's

office (i.e., 942, 947, 702, etc.).

(4) The next two (2) characters (alpha) are the user's first name and last name initials. When necessary this can be different to avoid duplication of user-IDs.

2.2.3 Generic and Service Account User-IDs: Generic account and service account user-IDs are established for special-purpose requirements. Examples where generic user-IDs may be used are to support training classes (TRAIN01, TRAIN02, etc.) or running computer jobs or testing for computer applications in test environments (RCIUSR1, RCIUSR2), sharing files for an office (FISCAL01, FDOTPIO, etc.), and kiosk computers used for public access. Service accounts are non-interactive accounts used by a system or application (e.g. service, scheduled task, batch process, etc.). Requirements for generic and service account user-IDs are as follows:

(1) User-ID naming conventions for generic and service account user-IDs shall be different from standard user-ID naming conventions so that they can be readily identified. These user-IDs shall be as descriptive as possible to associate the user-ID with the intended function.

(2) If a RACF account and an AD account are needed, then they should be named identically. If only an AD account is needed, and the user-ID requires more than eight (8) characters, then no RACF account should be created, and the AARF request should have YES in the Exception Request field with a justification.

(3) Users shall request ~~generic~~ these user-IDs via the AARF System. Information requirements ~~for generic user-ID requests~~ shall include account owner information, security groups or users with knowledge of this account, application name (for service use accounts), any applicable exemptions, interactive logon, mail accounts, logon hours, and the machine name(s) upon which the account shall be restricted for use. Users requiring assistance completing the AARF request for these special user-IDs should contact the FDOT Service Desk to submit a ticket for assistance. Exemptions to certain standards, such as password expiration, interactive logon, RACF exception, account disabled, and internet restriction, require approval from the ISM via the AARF request.

(4) Generic user-IDs used for training classes and testing computer applications must have restricted access controls in place to prevent unauthorized use once the training is completed.

(5) The users responsible for these ~~generic~~ accounts ~~user-ID is~~are also responsible for requesting the deletion of the user-IDs via the AARF system when it is no longer needed.

2.2.4 Corporate User-IDs: Corporate user-IDs are assigned to specific individuals and are used exclusively by that individual for access to the information technology resources titled Consultant Invoice Transmittal System (CITS). A ***Consultant Invoice Transmittal System Corporate Access Account Agreement*** is required in order to process the request for a corporate user-ID. Corporate user-IDs shall use the following naming conventions:

(1) User-IDs shall consist of ~~a minimum of~~ seven (7) ~~, maximum of eight (8)~~ characters (alphanumeric).

(2) The first two (2) characters (alpha) are the identification that the user is a corporate user. The first two (2) characters will always be IT.

(3) The next three (3) characters (alpha) are the designated initials of the user's company (i.e., TIE (Tierra, Inc.), PBS (PBS&J), etc.).

(4) The last two (2) characters (numeric) are the next sequential number available for that company (ITPBS01, ITPBS02, ITPBS03, etc.).

2.2.5 Outside Agency ~~(OA)~~ User-IDs: The FDOT Enterprise Security Team maintains a list of Florida and non-Florida Government Agencies with approved access to FDOT resources. Outside agency user-IDs are assigned to specific individuals and are used exclusively by that individual for accessing the Department's information technology resources. Outside agency user-IDs shall use the following naming conventions:

Formatted: Font: Not Bold

(1) User-IDs shall consist of seven (7) characters (alpha only).

(2) The first two (2) characters are the identification that the user is an outside agency user. The first two (2) characters will always be OA.

(3) The next three (3) characters are the designated initials of the user's agency (i.e., JTA (Jacksonville Transit Authority), FHW (Federal Highway Administration), etc.).

(4) The last two (2) characters are the user's first name and last name initials. When necessary this can be different to avoid duplication of user-IDs.

(5) An account expiration date must be entered in AARF for AD and RACF. If no expiration date is listed, the default revoke date of July 1 of the next fiscal year plus 2 years should be used.

2.2.6 Consultant User-IDs: Consultant user-IDs are assigned to specific individuals and are used exclusively by that individual for access to computer network resources. Consultant user-IDs shall use the following naming conventions:

(1) User-IDs shall consist of seven (7) characters (alphanumeric ~~only~~).

(2) The first two (2) characters are the identification that the user is a consultant. The first two (2) characters will always be KN.

(3) The next three (3) characters are the designated initials of the user's company (i.e., SSI (Skill Storm, Inc.), PBS (PBS&J), etc.).

~~(4)~~ The last two (2) characters are the user's first name and last name initials. When necessary this can be different to avoid duplication of user-IDs.

(4)

(5) An account expiration date must be entered in AARF and used for AD and RACF.

2.2.7 ~~Special~~ Separate Access User-IDs (FTP ~~-~~ Only): File Transfer Protocol (FTP) only user-IDs are assigned to specific individuals and are used exclusively by that individual for access to the computer network resource entitled the FTPEXT server. This account is strictly for users who only need FTP access and no other RACF or AD access. An FTP Addendum is required in order to process the request for an FTP only user-ID. The external FTP server, FTPEXT is a separate system from the internal ftp server, fdotftp.fdot.state.fl.us, which runs from the mainframe.

FTP only user-IDs shall use the following naming conventions:

(1) User-IDs shall consist of seven (7) characters (alphanumeric).

(2) External FTP ~~-~~only user IDs are defined as the following example, F###001 where F=FTP, ### = Cost Center, and 001 is an incremental counter for each external user in the cost center.

(3) No user shall have more than one user ID.

Formatted: Indent: Left: 0.5", Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

~~(3)~~(4) If the user obtains a RACF or AD account at a later time, then an AARF Transfer request should be submitted. The FTP-Only access will change to FTP access, and the FTP addendum must be completed. The RACF/AD userid will be used to create the FTP account although FTP is a separate system from RACF/AD.

2.2.8 ~~Special~~ Separate Access User-IDs (FTA ~~-~~Only): File Transfer Appliance (FTA)~~-~~only user-IDs are assigned to specific individuals and are used exclusively by that individual for access. FTA~~-~~only users are only authorized to send secured documents to FDOT email addresses. This account is strictly for users who only need FTA access and no other RACF or AD access. An FTA Addendum is required to process the request for FTA access. FTA~~-~~only user-IDs shall use the following naming conventions:

~~(1)~~ User-IDs shall consist of nine (9) characters (alphanumeric).

(2) FTA only user IDs are defined as the following example, FTA###001 where ### = Cost Center and 001 is an incremental counter for each external user in the cost center.

(2)(3) If the user obtains a RACF or AD account at a later time, then an AARF Transfer request should be submitted so that the FTA access can be documented under the newly assigned RACF or AD user-ID.

2.2.9 Special Office 365 Cloud-Only Access User-IDs (ITS/RTMCOffice 365-Cloud Only): Intelligent Transportation Systems (ITS) / Regional Transportation Management Center (RTMC) Office 365 -Cloud- Only user-IDs are assigned to specific individuals and are used exclusively by that individual for access to the Department's technology resources. These users are ITS/RTMC Intelligent Transportation Systems (ITS) / Regional Transportation Management Centers (RTMC) staff. This account is strictly for users who only need an Office 365 license and no other RACF or AD access. This license grants access for email, Sharepoint, etc. Office 365-Cloud Only user-IDs shall use the following naming conventions and guidelines:

(1) User-IDs shall consist of nine (9) characters (alphanumeric).

(2) Office 365-Cloud Only user IDs are defined as the following example: MSO###001, where ### = Cost Center, and 001 is an incremental counter for each external user in the cost center.

(3) If the user obtains a RACF or AD account at a later time, then an AARF Transfer request should be submitted so that the Office 365-Cloud Only access is removed, and a standard user ID is assigned with an email license associated with the AD account.

(4) Do NOT choose the Office 365-Cloud Only item:

(A) If the user has an existing AD account. The "Email" item should be chosen instead.

(B) If the user has an existing RACF account. An AD account should be created, and the "Network Access" and "Email" items should be chosen.

2.2.10 Office 365 Cloud-Only User-IDs (Resources and Shared Mailboxes): Mailboxes that are created in the Office 365 tenant for Resources (conference rooms and equipment) and Shared use. These Mailboxes shall use the following naming

Formatted: Font color: Black

Formatted: Keep with next

Formatted: Indent: Left: 0.5", Hanging: 0.5"

Formatted: Indent: Left: 1", Hanging: 0.38"

conventions:

(1) User-IDs in AARF shall consist of eleven (11) characters (alphanumeric). Note: There is no User-ID field within the Office 365 tenant when setting up mailboxes. The User-ID is assigned due to AARF system requirements.).

(2) Resource Mailboxes are defined as the following: MSODxRMB001, where Dx = District where the account is used, RMB indicates it's a Resource Mailbox, and 001 is an incremental counter for each mailbox in the district.

(3) Shared Mailboxes are defined as the following: MSODxSMB001, where Dx = District where the account is used, SMB indicates it's a Shared Mailbox, and 001 is an incremental counter for each mailbox in the district.

(4) The First Name field in AARF must match the first 25 characters of the Email Address assigned in the Office 365 tenant, up to but not including the @ symbol. For example:

(A) The user ID for FDOT-AARFStatewideAdministrators@dot.state.fl.us would be **FDOT-AARFStatewideAdminis**, since these are the first 25 characters before the @ symbol.

(B) The user ID for AARF-AccessItem@dot.state.fl.us would be **AARF-AccessItem**, since these are all the characters before the @ symbol.

2.2.11 Additional User-IDs (Test): Test user-IDs are assigned to specific individuals and are used exclusively by that individual's use for testing computer network resources. Test user-IDs shall not be used for production work and must use the following naming conventions:

(1) User-IDs shall match the naming convention of the user's assigned User-ID with an addition of an "T" at the end. For example:

(A) An FDOT employee is assigned a Standard User-ID of SS980XX, so the Test User-ID will be named SS980XXT.

(B) A Consultant is assigned a Consultant User-ID of KNABCYY, so the Test User-ID will be named KNABCYYT.

(C) An Outside Agency user is assigned an Outside Agency User-ID of

Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Underline
Formatted: Underline
Formatted: Font color: Black
Formatted: Default Paragraph Font, Font color: Black
Formatted: Font color: Black
Formatted: Font: Bold
Formatted: Font color: Black
Formatted: Font color: Black
Formatted: List Paragraph, Indent: Left: 1.38", First line: 0"
Formatted: Indent: Left: 1", Hanging: 0.38", Don't add space between paragraphs of the same style, Numbered + Level: 3 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1.38" + Indent at: 1.65"
Formatted: Default Paragraph Font, Font color: Black
Formatted: Font: Bold
Formatted: Font color: Black
Formatted: Font: Not Bold
Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Font: Not Bold
Formatted: Indent: Left: 1", Hanging: 0.38"
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold

OASRCZZ, so the Test User-ID will be named OASRCZZT.

(2) A corresponding RACF User-ID shall not be created, since TSO access cannot be granted to 8-character RACF user profiles. If a RACF account is required, then it will be named similarly to the user's assigned User-ID (such SS980AX, KNABCDX, OASRCFX), where the last letter is changed to a rarely used letter (such as X, Y, Z, Q) to denote a different use for the account.

2.2.12 Additional User-IDs (Administrator): Administrator user-IDs are assigned to specific individuals and are used exclusively by that individual for elevated access to computer network resources. Details regarding the responsibilities of this account type can be found in the Method and Practice document titled Active Directory Administrators' Roles and Responsibilities. Administrator user-IDs shall use the following naming conventions:

(1) User-IDs shall match the naming convention of the user's assigned User-ID with an addition of an "A" at the end. For example:

(A) An FDOT employee is assigned a Standard User-ID of SS980XX, so the Administrator User-ID will be named SS980XXA.

(B) A Consultant is assigned a Consultant User-ID of KNABCYY, so the Administrator User-ID will be named KNABCYYA.

(C) An Outside Agency user is assigned an Outside Agency User-ID of OASRCZZ, so the Administrator User-ID will be named OASRCZZA.

(2) A corresponding RACF User-ID shall not be created.

2.2.13 Additional User-IDs (Enterprise Administrator): Enterprise Administrator user-IDs are assigned to specific individuals and are used exclusively by that individual for elevated access to enterprise computer network resources. Details regarding the responsibilities of this account type can be found in the Method and Practice document titled Active Directory Administrators' Roles and Responsibilities. Enterprise Administrator user-IDs shall use the following naming conventions:

(1) User-IDs shall match the naming convention of the user's assigned User-ID with an addition of an "E" at the end. For example:

(A) An FDOT employee is assigned a Standard User-ID of SS980XX, so

Formatted: Font: Not Bold
Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Font: Not Bold
Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Font: Not Bold
Formatted: Indent: Left: 1", Hanging: 0.38"
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Indent: Left: 0.5", Hanging: 0.5"
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Indent: Left: 1", Hanging: 0.38"

the Enterprise Administrator User-ID will be named SS980XXE.

(B) A Consultant is assigned a Consultant User-ID of KNABCYY, so the Enterprise Administrator User-ID will be named KNABCYYE.

(C) An Outside Agency user is assigned an Outside Agency User-ID of OASRCZZ, so the Enterprise Administrator User-ID will be named OASRCZZE.

(2) A corresponding RACF User-ID shall not be created.

2.2.14 Additional User-IDs (Special Access): Special Access user-IDs are assigned to specific individuals and are used exclusively by that individual for access that would normally be restricted. Special Access user-IDs shall use the following naming conventions:

(1) User-IDs shall match the naming convention of the user's assigned User-ID with an addition of an "S" at the end. For example:

(A) An FDOT employee is assigned a Standard User-ID of SS980XX, so the Special Access User-ID will be named SS980XXS.

(B) A Consultant is assigned a Consultant User-ID of KNABCYY, so the Special Access User-ID will be named KNABCYYS.

(C) An Outside Agency user is assigned an Outside Agency User-ID of OASRCZZ, so the Special Access User-ID will be named OASRCZZS.

(2) A corresponding RACF User-ID shall not be created.

~~(B)~~

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font color: Black

Formatted: Normal, No bullets or numbering

2.3 ACCESS CONTROLS FOR PASSWORDS

2.3.1 This section applies to passwords that are required to access information technology resources within the Department at login. Other passwords exist as functional components within certain applications and are governed by the requirements of the individual application. The Department's ISM shall review and approve all

password schemas that govern the creation and assignment of user passwords where the password is used at login. A temporary password will be assigned to a new user in a manner that ensures the confidentiality of the password. This temporary password is required to be changed the first time the user logs on to the information resource.

2.3.2 Active Directory Password Requirements:

(1) Passwords must contain at least three of the four following characteristics:

(A) Upper case characters (A-Z)

(B) Lower case characters (a-z)

(C) Numbers (0-9)

(D) Special characters (@ # $)

(2) Active Directory passwords must be a minimum of eight (8) characters in length.

(3) The same password cannot be reused through 24 intervals of change.

(4) If ten (10) consecutive login attempts are made using the same user-ID with an invalid password, access for the user-ID will be revoked. Reinstatement of the access privileges for the user-ID is made by following the password reset process outlined in ***Section 2.3.4*** of this ***Manual Chapter***.

(5) Passwords have a lifetime of 65 days. In the case of sensitive data, passwords may be required to be changed more frequently. Requests for extended life or non-expiring passwords must be submitted via the AARF system. These exceptions require the approval of the ISM and must be attached to the AARF request prior to the request being finalized.

(6) Passwords that have been issued to and changed by a user shall not be shared.

(7) Passwords shall be protected against disclosure: memorized and not written down.

(8) User passwords shall not be stored or entered by automatic means, such as with macros.

2.3.3 RACF Password Requirements:

(1) Passwords must contain at least two of the three following characteristics:

(A) Alphabetic characters (A-Z)

(B) Numbers (0-9)

(C) Special characters (@ # $)

(2) RACF passwords must be between five (5) and eight (8) characters in length.

(3) The same password cannot be reused through 24 intervals of change.

(4) If five (5) consecutive login attempts are made using the same user-ID with an invalid password, access for the user-ID will be revoked. Reinstatement of the access privileges for the user-ID is made by following the password reset process outlined in ***Section 2.3.~~4~~ 5*** of this ***Manual Chapter***.

(5) All passwords have a lifetime of 65 days. In the case of sensitive data, passwords may be required to be changed more frequently. ~~In the case of corporate user IDs, passwords are assigned as non-expiring.~~ Requests for extended life or non-expiring passwords must be submitted via the AARF system. These exceptions require the approval of the ISM and must be attached to the AARF request prior to the request being finalized.

(6) Passwords shall not be shared.

(7) Passwords shall be protected against disclosure: memorized and not written down.

(8) User passwords shall not be stored or entered by automatic means, such as with macros.

2.3.4 FTP Server Password Requirements:

(1) Passwords must contain all the three following characteristics:

(A) At least one letter

(B) At least one number

(C) At least one special character

Formatted: Indent: Left: 1", Hanging: 0.5"

(2) FTP passwords established for Department-owned information resources must be a minimum of eight (8) characters in length.

(3) The same password cannot be reused through 24 intervals of change.

(4) If ten (10) consecutive login attempts are made using the same user-ID with an invalid password, access for the user-ID will be revoked. Reinstatement of the access privileges for the user-ID is made by following the password reset process outlined in ***Section 2.3.5*** of this ***Manual Chapter***.

(5) All passwords have a lifetime of 65 days.

(6) Passwords that have been issued to and changed by a user shall not be shared.

(7) Passwords shall be protected against disclosure: memorized and not written down.

(8) User's passwords shall not be stored or entered by automatic means, such as with macros.

2.3.5 Methods of Reset

The following options shall be the only means of requesting password resets for all accounts having access to the Department's information technology resources:

(1) **Identity Management:** All internal users should establish an account with the Department's password management system. Internal users without an established profile with the password management system may request assistance from the FDOT Service Desk. Instructions are also available on the Department's internal Computer Based Training (CBT) website. When creating a profile with the password management system, the user must provide a series of challenge questions and answers. Knowledge of these questions and answers enable the user to reset their password in the event the user's AD or RACF account becomes locked. Users may use "pwreset" as the username and password from the Windows logon screen to access the system to reset his or her own password.

~~(1)~~(2) **AD and RACF:** Password resets can be requested by contacting the Service Desk. Prior to resetting a user's password, every effort should be made to verify the user's identity.

To verify the user:

- The user must have knowledge of their RACF user-ID
- Confirm the user's status in AARF
- Confirm the user's email address in AARF
- Confirm the user's knowledge of their Supervisor or Project Manager's Name

Passwords may be emailed using the secured File Transfer Appliance (FTA) to the user's OIT Security Coordinator, immediate Supervisor, or the Project Manager. The user's OIT Security Coordinator, immediate Supervisor, or the Project Manager may also make a request for a password to be reset on behalf of the user.

~~(2)~~ **Corporate (CITS) Accounts Only:** User's knowledge of their Supervisor or Project Manager is not required since this does not apply to CITS-Only accounts. Passwords may be emailed using the secured File Transfer Appliance (FTA) to only the user.~~Password reset requests for corporate user accounts can be made by contacting the Service Desk. Corporate Account password reset requests sent to the Service Desk must only generate service desk tickets. These tickets are routed to the FDOT Enterprise Security team (CO ECS Main).~~

(3) ~~**Identity Management:** All internal users should establish an account with the Department's password management system. Internal users without an established profile with the password management system may request assistance from the FDOT Service Desk. Instructions are also available on the Department's internal Computer Based Training (CBT) website. When creating a profile with the password management system, the user must provide a series of challenge questions and answers. Knowledge of these questions and answers enable the user to reset their password in the event the user's AD or RACF account becomes locked. Users may use "pwrest" as the username and password from the Windows logon screen to access the system to reset his or her own password.~~

Formatted: Indent: Left: 0.5", Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 2 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.5", Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 3 + Alignment: Left + Aligned at: 2.25" + Indent at: 2.5"

Formatted: Indent: Left: 0.5", Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 3 + Alignment: Left + Aligned at: 2.25" + Indent at: 2.5", No widow/orphan control

(4) **External FTP Accounts:** FTP-Only and FTP accounts are reset by the FTP Administrator or by the user using the self-service option in the FTPEXT application. Passwords resets not made via the self-service option can be requested by contacting the Service Desk.

Formatted: Font: Bold

(5) **Generic/Service Accounts:** Password reset requests for generic/service accounts may be requested by contacting the Service Desk, telephone, or email. Generic/Service Account password reset requests sent to the Service Desk must only generate service desk tickets.

Formatted: Font: Bold

~~(4)~~

Formatted: No bullets or numbering

~~(5)~~ 2.4 NEW USER

2.4.1 All **new users** will receive the necessary documentation needed to request access to the Department's information resources from the OIT Security Coordinator, District IT Services Manager or designee. This documentation shall include security-related policies, procedures, manual chapters, forms, rules, standards, and applicable Florida Statutes and Florida Administrative Code.

2.4.2 The first step in obtaining any form of security access is the new user completion of the Technology Resource Awareness Certification Kit (T.R.A.C.K.) CBT and the submission of a request for access. ~~Agency for~~Division of State Technology (DA~~S~~ST) employees requesting access are authorized to submit the DA~~S~~ST Computer Security certificate of completion, in place of the FDOT T.R.A.C.K. CBT Certificate.

2.4.3 The cost center requesting the new user-ID shall initiate the request within the ~~Automated Access Request Form (~~AARF~~)~~ System. The request shall include any special instructions as well as additional information or attachments needed for access to the information resource. A list of **information resources** is included within the AARF System as well as provisions for special instructions, requirements, and comments. The OIT Security Coordinators or **FDOT Enterprise Security Team** can assist with initiating the request.

2.4.4 Upon the completion of the mandatory security awareness training, new users are required to sign ***Form No. 325-060-08, "Acceptable Use Agreement (AUA)"***,

available within the AARF System. Upon signing the AUA, the form and the user-signed T.R.A.C.K. CBT Certificate of Completion shall be attached to the user's AARF request. Once the request is finalized, the attached AUA becomes part of the user's security records. The AARF System shall utilize the signed AUA as the established signature on-file for subsequent access requests. The AARF request shall be finalized prior to granting access.

(1) The AARF System maintains signatures on file so access requests can be approved by supervisors, Cost Center Managers, and security coordinators electronically, without having to sign additional forms. All approving authorities shall have a signature on file prior to approving any access request.

(2) The following additional information is required for consultants, outside agencies, and other sources:

(A) For consultants, additional information, including the user's DOT Project Manager, consultant company name, vendor number or federal tax ID (FEID), consultant representative's name, project number, and project end date is required.

(B) For outside agencies, additional information, including the user's Agency name, and project end date is required.

(C) Access requests from any other source (general public, private sector, media, etc.) will be handled on a case-by-case basis involving coordination between the Department's Chief Information Officer (CIO), Public Information Office (PIO), Office of General Counsel (OGC), and the appropriate SMS-level manager. Generally, the Department is able to comply with public records requests without needing to grant outside access to our computer network resources.

2.4.5 Corporate access accounts are established for a company or consultant to access and utilize the CITS via the FDOT Network. Instructions are available on the Procurement website.

(1) All corporate access account requestors must:

(A) Establish account with the FDOT Central Office Procurement Office. The corporate executive must complete and sign the ***form No. 375-031-00, "Consultant Invoice Transmittal System Corporate Access Account Agreement"*** for initial account set up using the

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Docusign process.

(B) Request access with the FDOT Central Office Procurement Office. Company employees must complete and sign ***form No. 325-060-06, "FDOT Computer Security Access Request for Corporate Accounts"***.

(C) Complete the mandatory security awareness training within the previous 12 months and provide completion form to FDOT Security.

(2) The corporate access account will remain active. if thea password reset within the specified time and logon has occurred within the previous 18 months. The password is set to expire after 65 days inactivity. An account expiration date must be entered in RACF.

(3) The FDOT Enterprise Security Team shall provide the password to the user in a manner that ensures confidentiality.

(4) Requests for corporate accounts are not currently submitted through AARF.

2.4.6 In addition to ***Form No. 325-060-08***, ***"Acceptable Use Agreement (AUA)Form"*** and the T.R.A.C.K. CBT Certificate, requests for access to specific network resources as defined in ***Section 2.9*** of this ***Manual Chapter*** must be attached to the request. All enterprise applications that require authentication shall be requested via the AARF System.

2.4.7 Business Coordinators are included in the AARF System workflow. The business coordinators shall ensure:

(1) The AARF request includes all the required access, such as e-mail, Resource Access Control Facility (RACF), and Active Directory (AD), on an as needed basis, and that appropriate instructions and justifications are included on the final review page of the AARF request.

(2) The user-signed AUA and T.R.A.C.K. CBT certificate areis attached to the AARF request.

(3) The T.R.A.C.K. CBT Certificate is attached to the AARF request, and attach the certificate.

(4)(3) The AARF request is modified as necessary to ensure completeness and accuracy, including uploading needed attachments.

~~(5)~~(4) The request is approved and submitted to the OIT Ss~~s~~ecurity Coordinators for processing.

~~(6)~~(5) The FDOT Enterprise Security Team or the District OIT Security Office, shall reject the request as necessary. The rejection notification will be automatically emailed to previous approvers with the ~~-~~reasons for the rejection.

2.4.8 Upon notification of the receipt of an AARF request, the OIT security coordinators responsible for processing the request shall:

(1) Ensure the completeness and accuracy of the AARF request.

(2) Communicate with the user, user's supervisor, user's Cost Center Manager, user's Business Coordinator, or with the FDOT Enterprise Security Team to resolve discrepancies.

(3) Modify and notate the AARF request as necessary to ensure appropriate accesses and justifications are in place.

(4) Assign the new user a RACF user-ID as described in ***Section 2.6*** of this ***Manual Chapter***.

(5) Approve or reject the AARF request as appropriate.

2.4.9 The District or Central Office IT Services Manager is ultimately responsible for ensuring the finalization of the user's AARF request and the issuance of the user's RACF and Network user-ID and first-time password within two (2) business days of OIT receipt of the completed request.

2.4.10 Once the user's District OIT security office finalizes the user's AARF request, the AARF System automatically notifies the appropriate Functional Application Owners that the user has requested access to a system. Functional Application Owners and/or Access Coordinators shall appropriately acknowledge in AARF that the access has been granted or reject the item and state the ~~notify the FDOT Enterprise Security Team of their rejection and~~ reason for rejection.

2.4.11 All forms, attachments, access requests, and access terminations shall be maintained within the AARF System in accordance with the State of Florida's general records retention requirements.

2.4.12 The ISM is responsible for facilitating the maintenance of access requests. Therefore, the ISM shall ensure the AARF System processes access and termination requests appropriately and in accordance with State of Florida guidelines, statutes, and

administrative rules.

2.5 TRANSFERRED USER

2.5.1 When a transfer request is submitted, it is processed as a termination of original access and establishment of new access. When it is finalized, the new account will be created, tThe old account will be revoked/disabled, and the new accountapplication owners shall revoke access within two (2) business days of the effective date as noted in AARF or upon receipt of the request, whichever is later will be created. Additionally, the finalization of a transfer request within the AARF System effectively transfers the user's computer security access records to the new cost center.

2.5.2 A transfer request shall be submitted via the AARF System:

(1) For users/accounts changing cost centers or districts. If the change in cost centers is due to a Departmental reorganization, where there is no change in job duties, then the existing user-IDs are not required to be changed.

(2) For consultants leaving one company and being hired with a different company. The old account will be revoked/disabled, and the new account will be created using the naming convention for the new company. Consultants who augment staff may be renamed if the duties and accesses will not change.

(3) For users changing Account Types (Employee/OPS to Consultant/Contractor or vice versa).

(4) For users who have been terminated within 13 months and are returning to active status.

2.5.3 The office to which the user is transferring must initiate the transfer request by the effective date or receipt of the transfer, whichever is later. The new account shall be created in accordance with ***Section 2.4*** of this ***Manual Chapter.*** Upon the effective date of the transfer, the previous user-ID associated with the user's employment shall be immediately disabled and then terminated in accordance with ***Section 2.6*** of this ***Manual Chapter***. Requests for exceptions to this requirement shall be submitted to **FDOT Security** for the initial review. FDOT Enterprise Security Team will vet the request and contact the ISM for approval.

2.5.4 District Transfer requirements for the District IT Security office to which the user

is transferring:

(1) Coordinates the transition of email and/or files.

(2) Requests ~~Call~~ Cost Center Manager approvals for retaining email archive.

2.5.5 Cost Center Transfer requirements for the District IT Security office:

(1) Coordinates the transition of email and/or files.

(2) Requests Cost Center Manager approvals for retaining email archive.

2.6 TERMINATED USER

2.6.1 When an employee terminates his or her employment or contract with the Department, the employee's Cost Center Manager shall ensure that a termination request is submitted via the AARF System. All termination requests shall be initiated by the user's business unit and approved by the Cost Center Manager in the AARF System no later than the user's separation date.

2.6.2 All termination requests shall be processed and finalized by OIT Security, application owners notified, and access revoked within two (2) business days of the effective date as noted in AARF or upon receipt of the request, whichever is later.

2.6.3 Under emergency circumstances, a Supervisor or Cost Center Manager may contact OIT Security to immediately terminate a user's access to the Department's technology resources. Regardless of the method of contact for an emergency termination (phone, email, in-person, etc.), a follow-up AARF request is required. The actual notification date should be included on section six (6) of the Human Resources ***Form No. 250-005-25, Notice of Separation/Resignation***.

2.6.4 A consultant's user-ID shall not be valid after the project end date of the consultant's assigned project. The project end date shall be entered into the AARF System on the Consultant Information Addendum page. The Project Manager is responsible for updating the consultant's AARF records when:

(1) The project end date is extended

(2) The consultant changes companies

(3) The project is completed

(4) The user-ID is no longer needed

~~**2.6.5** Under emergency circumstances, a Supervisor or Cost Center Manager may contact OIT Security to immediately terminate a user's access to the Department's technology resources. Regardless of the method of contact for an emergency termination (phone, email, in-person, etc.) a follow-up AARF is required. The actual notification date should be included on ***Section 6*** of the ***Human Resources Form No. 250-005-06, "Notice of Separation/Resignation"***.~~

2.6.~~6~~5 The terminated user's supervisor or Project Manager shall be responsible for ensuring any files that were maintained by the terminated user are copied and archived as necessary within 30 days of separation. The Cost Center Manager, supervisor, or Project Manager may request an extension to the 30-day deadline if necessary to ensure no loss of valued Department resources.~~The terminated user's supervisor or Project Manager shall be responsible for ensuring any files that were maintained by the terminated user are copied and archived as necessary within 30 days of separation.~~

2.6.~~7~~6 After access has been terminated, the associated access request forms and other access documentation shall be maintained for thirteen (13) months from the separation date to meet the State's current records retention requirements.

2.6.~~8~~7 If a terminated user has a record in AARF, a Transfer request must be submitted to reactivate the record. This maintains access history for the user under one record.

2.6.~~9~~8 ~~The RACF and AD accounts of terminated users will be deleted after 30 days have passed since the separation date. The RACF accounts are deleted via a deletion script run on the last Tuesday of the month. The AD accounts will be deleted after 30 days from the separation date.~~The RACF and AD accounts of terminated users will be deleted ~~monthly. The RACF accounts are deleted via deletion script on the last Tuesday of the month. The AD accounts will be deleted after~~ 30 days after ~~from~~ the separation date.

2.6.9 When applicable, the Application Services Office ~~OIT Security~~ will create a service ticket for the Division of State Technology to remove PanAPT access 30 days after the separation date.

Formatted: Font: Bold

2.7 Access to other Information Technology Resources

2.7.1 Users must have an established RACF user-ID as described in ***Section 2.4*** of this ***Manual Chapter***.

2.7.2 For additional access, an Access Change request shall be submitted via the AARF System. The request shall include any special instructions as well as additional information or attachments needed for access to the resource. A list of items are included within the AARF System as well as provisions for special instructions, requirements, and comments.

2.7.3 Cross District Access request must be submitted via the AARF system when additional access is needed to a different district's resources. The request must be submitted by someone who has access to initiate requests for that district. The request shall include any special instructions as well as additional information or attachments needed for access to the resource.

2.7.4 After granting access to the user and providing instructions, the Functional Application Owner shall acknowledge the access within the AARF System as specified in ***Section 2.4*** of this ***Manual Chapter***.
2.7.5 After removing access for a terminated user, the Functional Application Owner shall acknowledge the access within the AARF System as specified in ***Section 2.6*** of this ***Manual Chapter***.

2.8 SPECIAL ACCESS CONSIDERATIONS

2.8.1 FTP services are available within the Department for the **Internal** and **External** use. The External FTP server requires a secured logon for users uploading data to the server. A guest logon is available for downloading only. General information about using FTP services can be obtained by contacting the FDOT Enterprise Security Team or the FDOT Service Desk. Internal FTP services are available to all FDOT users with Active Directory access.

2.8.2 The Department provides a File Transfer Appliance (FTA) service. The FTA is a secure and encrypted method of electronically transferring files, folders, and programs. FTA services are available to all FDOT users with an FDOT email address. Users without an FDOT email address may request this access via the AARF system. For ~~one time~~one-time file transfers, an FTA user may use the Request File option to generate a link that will allow a single use transfer to occur within 10 days. This temporary access does not require an AARF request.

2.8.3 Internet Subscriber Account (ISA) – The ISA system is a subscription login component that authenticates external users and provides access to certain FDOT applications based on application role assignment. The system supports external users of Department's Internet applications that do not need or have access to any of the Department's internal systems or network.

The ISA system must only be used to authenticate users that:

- Do not have or need RACF accounts.
- Only need access to non-confidential information.
- Need only internet access to the Department's internet information resources.

2.8.4 FLAIR Access Security

For requirements concerning FLAIR access security, refer to ***Topic No. 350-090-150***, ***FLAIR Access Security***.

2.9 VALIDATION AND RE-CERTIFICATION

2.9.1 Recertification is the process by which access to specific information technology resources are validated and, if determined necessary, updated. FDOT's annual recertification confirms the Department's compliance to Florida Administrative Code 74GG-2 and Florida Statute 282.318 that directs agencies to ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. The Department's annual review of access to Information Technology resources serves to safeguard the Department's data and to prevent unauthorized access, ensure integrity and to mitigate risks.

2.9.2 User access records shall be provided to all Cost Center Managers with users, by the FDOT Enterprise Security Team. Cost Center Managers shall validate their employees' access privileges and re-certify that the user-IDs are valid and access privileges are appropriate. Cost Center Managers shall ensure that any required changes to access are submitted in the AARF system. The FDOT Enterprise Security Team shall work with each Districts' OIT security office to facilitate the update of access records indicated by the Cost Center Manager's approved AARF recertification request.

2.9.3. Application review requests may be requested by the Functional Application owners to the FDOT Enterprise Security Team. Functional Application Owners are responsible for determining the review cycle specific to their resource and conducting periodic reviews. Application reviews must include the validation of users with access and level of access that has been approved on the user's security records in AARF.

OIT serves as the Functional Application Owners for the following systems and these accesses shall be reviewed annually:

(1) CITS Corporate User-IDs

(2) External FTP

(3) RACF

(4) AD

2.9.4 Additionally, if the results of a quality assurance review or formal audit indicate the files maintained by the District IT Services Manager or the ISM are not complete or current, a re-certification process shall be required for the area being reviewed or audited. This will be done by requiring all approval forms to be resubmitted for approval signatures. Copies of previously submitted forms are unacceptable. All processes

outlined in this procedure for obtaining approval signatures on the required forms will be included in the re-certification process.

2.10 COMPLIANCE

Misuse or abuse of information technology resources is subject to the Department's disciplinary standards, up to and including immediate dismissal, civil penalties, or criminal penalties. Refer to the Department's ***Disciplinary Standards*** contained in ***Rule 60L-36.005, Florida Administrative Code*, and *Topic No. 250-012-011, Disciplinary Action***. Additionally, failure to comply with related department policies, procedures, and standards may lead to termination of contracts for contractors, partners, consultants and other entities that provide a service to the department. Furthermore, pursuant to ***Chapter 815, F.S.***, ***Computer Related Crimes***, all individuals who violate these related statutes, rules, policies, procedures, and standards, are subject to possible legal (civil and/or criminal) prosecution pursuant to applicable ***Florida Statutes***.

TRAINING:

The Technology Resource Awareness Certification Kit (T.R.A.C.K.) CBT ~~Computer-based security awareness training~~ is required for all new user requests. ~~This awareness training is available on the , located on the Department's Intranet (FDOT Employee Portal) and Internet sites. Information about how to obtain this training is available from the Information Security Manager (ISM) or the District IT Services Manager.~~ The Information Security Manager (ISM) is responsible for developing, maintaining, and distributing the course instructions. Additionally, users shall complete the T.R.A.C.K. ~~computer security~~ training on an annual basis via Learning Curve (for FDOT employees) or on the FDOT website under the Information Security Administration section.~~or the external website.~~

FORMS:

Form No. 325-060-08, Acceptable Use Agreement (AUA)
Form No. 325-060-06, FDOT Computer Security Access Request (CSAR) for Corporate Accounts
Form No. 375-031-00, Consultant Invoice Transmittal System Corporate Access Account Agreement
Form No. 250-005-25, Notice of Separation/Resignation