

User Account Management (UAM) Guide

1 June 2009

Prepared By
Dr. Clifton Stine
PM TIS Technical Director
Version 1

Table of Contents

1.0 Introduction	3
2.0 The UAM	3
2.1 The Purpose of the UAM	3
2.2 UAM Appointment	4
3.0 User Account Creation	4
4.0. Account Maintenance.....	5
5.0 Reset User's PM TIS Portal Password	6
6.0 Delete PM TIS User Account.....	6
7.0 Enable/Disable PM TIS User Account.....	6
8.0 Contacting PM TIS.....	6

PM TIS User Account Management Policy

1.0 Introduction

This document establishes the user account management process for the Product Manager, Transportation Information Systems (PM TIS) Enterprise system. This process covers all aspects of the user account management requirements, including the appointment of the User Account Manager (UAM), and the creation, deletion, and modification of CITRIX and Transportation Coordinators' – Automated for Information Movements System II (TC-AIMS II) Enterprise user accounts.

The procedures defined in this policy relate specifically to Enterprise operations.

Individuals involved in the user account management process are identified below:

- TIS User – End user of the TC-AIMS II application hosted on the PM TIS Enterprise.
- UAM – A trusted TIS agent at a local installation that has been granted the authority to authorize and facilitate the creation, maintenance, and overall management of PM TIS accounts and application profiles for a defined user population (e.g., for users belonging to a defined set of units/Unit Identification Codes (UICs))
- PM TIS Customer Service Center (CSC) – Consists of CSC personnel who assist customers with the account creation, maintenance, and/or deletion.
- Approval Authority – The commander of the Brigade or equivalent level specific military unit (or their official designee), that can appoint UAMs, authorize user access to the TC-AIMS II Enterprise application and to a unit's UICs, and data within the application.
- Security Officer – Appointed security officer at a local installation that can verify and maintain the background investigation/ADP level of individuals requesting access to the PM TIS Enterprise.

2.0 The UAM

Units throughout the Armed Forces must be prepared to deploy and fulfill their operational missions at all times. To successfully accomplish this task, units must have trained system operators to manipulate operational data and ensure deployment requirements are met. To decentralize the TIS responsibility of establishing accounts for unit system users, the UAM was created.

2.1 The Purpose of the UAM

The UAM serves as the primary point of contact for the creation and maintenance of the PM TIS Enterprise accounts for the unit level users. The UAM is responsible for creating, modifying, deleting, assigning, and verifying the positive identification of all designated users and possesses administrative control of all subordinate unit UICs and access to unit data.

2.2 UAM Appointment

UAMs are required for all installations/organizations that use the PM TIS Enterprise applications. UAMs are designated at Brigade (or equivalent) level units and organizations. To ensure proper operational coverage and redundancy, PM TIS recommends that at least two (but no more than three) UAMs be appointed for each Brigade. UAMs are appointed via the UAM Appointment Memorandum. This appointment memorandum specifies the name, rank, SSN, AKO email address, and phone number of each UAM being appointed and their signature, as well as the list of UICs for which each UAM is responsible. The memorandum must be signed by the Brigade-level (O-6) commander equivalent (e.g., GS-15). Navy UAMs must be appointed by an O-5 or their equivalent. Exceptions for the O-6 signature requirement will be reviewed on a case-by-case basis for Detachments and/or smaller organizations that do not correlate directly to a Brigade level command. For these cases, the highest level commander can act as the approval authority for the appointment of their UAMs. Upon completion, the UAM appointment will be sent to the CSC via fax or email.

3.0 User Account Creation

The steps for obtaining an account are outlined below:

Step 1. Download the PM TIS Enterprise Account Request Form (EARF) from the PM TIS Web site: <https://www.tis.army.mil/fielding-docs.htm>.

Step 2. The UAM completes and signs the EARF, then sends it via email to PM TIS Security (kacey.faircloth@us.army.mil) and the CSC (tishelpdesk@conus.army.mil) or fax (703-752-1450).

Note: The EARF requires an email address for both the user and the UAM for their AKO or Navy Marine Corps Intranet (NMCI) email addresses. This relates specifically to Army, Navy, and Marine Corps users. This information is vital to the account creation process.

Step 3. Security.

- a. The UAM will provide the unit security officer with appropriate levels required to support PM TIS.
- b. The unit security officer will verify that the individuals selected to support PM TIS are cleared at the appropriate level.

Step 4. While Security is verifying this information, the CSC will verify that the EARF has been completed correctly. If any information is missing or illegible, the CSC will contact the UAM and ask them to re-submit the EARF with the necessary corrections.

Step 5. Security will notify the CSC when the user does not have the appropriate level clearance or background investigation. At a minimum, a National Agency Check (NAC) is

required. The CSC will notify the UAM that the user's accounts cannot be created and provide the reason for the denial.

Step 6. Once an account has been created, the CSC will send the login credentials to the user's email address as specified on the form. User IDs and passwords are sent in separate emails to ensure proper information security is maintained.

4.0. Account Maintenance

TC-AIMS Enterprise users require a process to make changes to their accounts. To facilitate this process, PM TIS has published the Enterprise Account Change Request Form (EACRF). This form is available on the PM TIS Web site and may be completed by the TC-AIMS Enterprise user requiring the modifications to their account. To ensure that the change requested is appropriate for the user, the UAM must sign the request.

Upon completion, the EACRF will be sent to the CSC via fax or email. The EACRF does not require any action by PM TIS Security. The EACRF options that a TC-AIMS Enterprise user may request are listed below:

Add Access to Existing PM TIS User Account

This process would be used to grant an Enterprise user with an existing PM TIS user account additional access to applications, UICs, and/or profiles. PM TIS users may only request the addition of applications, UICs, and/or profiles to their own account.

Change Access for an Existing PM TIS User Account

Under this process, access within a PM TIS Enterprise account (application, UIC, or profile) can be changed. This process can be used to exchange access within PM TIS applications, users will only be able to request changes to their own accounts. The PM TIS Enterprise user can initiate the deletion of an application from their account (and only from their account) by logging into the portal and completing an on-line form available within the portal. UAMs will also have the ability to initiate the deletion of an application from a PM TIS user account within their defined user community

Existing PM TIS User Account Access Elimination

This process is used to eliminate access to applications, UICs, and/or profiles for an existing user account. To protect against accidental or erroneous application account deletions, the account will initially be disabled for a period of 15 days before access to it is permanently removed. PM TIS users may only request the removal of applications, UICs, and/or profiles to their own PM TIS account.

5.0 Reset User's PM TIS Portal Password

If a user needs a password reset for either a CITRIX account or a TC-AIMS account, the user will need to contact the CSC via telephone, fax, or email. Positive identification of the requesting individual is verified prior to password reset. The new password information will be sent to the individual's designated email account.

6.0 Delete PM TIS User Account

Deleting a PM TIS user account involves deleting the user's portal (i.e., Citrix) account, as well as deleting all of the individual's application accounts (e.g., TC-AIMS II, AALPS). The PM TIS end user can initiate the deletion of his own account (and only his own account) by completing the EACRF. UAMs may initiate the deletion of PM TIS user accounts within their defined user community. Bulk account deletions can be processed using the EACRF with an additional sheet specifying the users to be deleted included. Accounts will be deactivated after 45 days and deleted after 18 months.

To protect against accidental account deletions, the account will initially be disabled for a period of 15 days before it is permanently deleted.

7.0 Enable/Disable PM TIS User Account

UAMs may initiate the disabling/enabling of PM TIS user accounts within their defined user community. Bulk account enabling/disabling can be processed using the EACRF with an additional sheet specifying the users to be enabled/disabled included.

8.0 Contacting PM TIS

The Customer Service Center can be contacted using the following methods:

Phone:

Toll Free Phone: 1 (866) 822-4672

Direct: (703) 752-0806

DSN: (312) 221-5000

Email:

tishelpdesk@conus.army.mil

Fax:

(703) 752-0737

Please do not hesitate to contact us if you have any questions or concerns reference user account management