Read Me First

Introduction to e-ISuite

Overview

User Resources: e-ISuite Website -- http://famit.nwcg.gov/applications/eISuite

Various training materials are available for students in several formats. These materials have been developed to accommodate student preferences for first time learning or refreshing on user roles and functional areas. All materials are easily accessible on the e-ISuite website.

- Helpful Resources – This link provides a listing of documents containing supplemental information for students, from a Site installation PPT to tips for writing custom reports.

- User Guides -- User Guides are available on the website.
  - User Guides can be printed by clicking on the appropriate links on the website.

- On-Line Tutorials – These sessions are automated/narrated short courses which can be downloaded and viewed to fit user needs. Specifics on software and computer requirements to view these sessions are outlined.
  - Students can locate and track their progress through the on-line Table of Contents.
  - These can be used as refreshers.

- Quick Reference Cards (QRCs) – These "cards" provide streamlined information on important topics.

Where to Get HELP

- On-Line Help System – This is the On-Line Help function within the application, searchable by very specific topics within the system. Click the HELP button on the Home Page (upper right corner), then search by topic.

  - If you are at an incident, contact the incident ITSS.
  - For additional help, contact the e-ISuite Help Desk.

- The e-ISuite website contains a wide variety of documentation, including:

  - ROSS Import
  - Updates
  - NAP Account Information

System Differences:

Enterprise:

- Web-based – Internet required
- Typically used for Initial Attack, ABCD Misc, S&R, Training Support, Dispatch and Cache Support
- Type 3, 4 & 5 Incidents
- Housed at central location in Kansas City, MO
- Eventually interface with other systems: ROSS, ICBS-R, agency payment centers
- NAP account required for all users.

Site:

- Installed on local incident server only – internet not required
- Incident may begin at Enterprise and transition to Site
- Type 1, 2 & 3 incidents
- All Site data transferred to Enterprise at incident closing
- NAP account not needed.

e-ISuite Roles/Functional Areas Quick Overview

Roles:

Account Manager

- Creates user accounts.
- Assigns user Non-Privileged/Privileged roles.
- Administers and monitors user accounts.
- Resets user passwords
- Creates initial Site Account Manager Account

Data Steward

- Creates and administers incidents/incident groups
- Assigns/imports users/user groups to incidents.
- Imports existing ROSS databases to e-ISuite
- Administers the Financial Export function.
- Administers Data Transfer actions.

Check-in/Demob

- Add/edit/delete/roster resources.
- Prepares resources for demob.
- Have access to Common Data section and functional section.

IAP

- Creates the Incident Action Plan.

Time

- Manages time records, creates payment documents and reports.

Cost

- Analyzes and reports cost data.

TNSP (Training Specialist) (NEW)

- TNSP tracking of incident trainee assignments and provides forms generation.

Read Me First

Functional Areas:

Incidents Button

- Is a function of the Data Steward Role which can add/edit/delete incidents and incident groups.

Check-in/Demob Buttons

- Check-in enters resource data.
- Demob prepares resources for release from an incident.
- Together have same access to screens, same permissions, can add and edit both functions.

IAP Button

- IAP uses database information to create ICS forms for an Incident Action Plan.
- The user can create the following ICS forms in IAP: ICS202, ICS203, ICS204, ICS205, ICS206 and ICS220.
    - Create, copy, delete forms and plans.
    - Import PDFs to be added to a plan.
    - Export plan files.
    - Form data is input using drop-downs and lists which will be inserted/formatted in each form.
    - Depending on the amount of form data, the printed form will be adjusted to create form page(s) with complete data (headers/footers).

Time Button

- Time allows the user to manage time records, create payment documents and reports.

  Use this to:
    - Post personnel, crew, and contract time.
    - Post commissary adjustments.
    - Edit roster data.
    - Print invoices (OF-286 and OF-288).

Cost Button

- Cost is a tool to analyze and report cost data.

  Use this to:
    - Generate daily cost records.
    - View daily cost records.
    - Edit daily cost records.

Training Specialist Button (NEW)

- Tracks incident trainee assignment(s).
- Tracks Evaluator data and work with trainees.
- Provides all forms, reports and statistics.

Reports Button

Each functional area (Check-in/Demob, Time and Cost) has specific reports associated with it. These reports will be covered under each functional area during the course.

Custom Report Button:

- Allows users to create non-standard reports.

Security:

Rules of Behavior:

All e-ISuite users must understand and follow the Rules of Behavior, the security principles and practices, and know and practice their responsibilities regarding e-ISuite security.

> **NOTE:** Some Incident Management Teams have a Rules of Behavior document that must be read and signed.

It is everyone's responsibility to safeguard the information that is collected, stored and maintained by the e-ISuite application.

The Rules of Behavior do not replace but enhance existing agency policies.

Users are to work within the confines of their authorized access or role. Users should not attempt to access other modules or screens in the e-ISuite application to which they do not have authorization. User accounts and additional roles can be granted by a user with an **Account Manager** role.

Security violations include, but are not limited to:

- Sharing of user name and password pairs.
- Sharing e-ISuite information or data with individuals who do not have an official need to know.
- Violating any other security policy or procedure.

If you leave your computer for any period of time, close the e-ISuite application. This will ensure that no unauthorized person can access the e-ISuite application while you are away.

e-ISuite Security Principles:

An Enterprise user must have a NAP account for access to e-ISuite Enterprise.

A Site user must have an active user account in a Site e-ISuite system in order to log into the Site e-ISuite application. The only exception to this rule is during the initial setup procedure when an initial **Account Manager** account is created. Each user must be assigned a unique user name and password to log into an e-ISuite Site system.

Only a user with **Account Manager** role can create User Accounts.

The e-ISuite application includes an automatic backup feature that allows backup of the database as often as needed.

The Data Steward role performs the following:

- Create a new database.
- Copy an existing database.
- Switch between multiple databases.
- Edit a database.
- Perform a manual backup.
- Perform an Automatic Backup.
- Restore a database.
- Remove a database.

The requirements for a database password are:

- Must contain a minimum of 12 characters.
- Must contain at least 1 lowercase letter.
- Must contain at least 1 uppercase letter.
- Must contain at least 1 number.
- Must contain at least one of the following special characters:
    - !#%&*^
- Cannot be a dictionary word.

e-ISuite databases should NOT be distributed to anyone except those outlined in other policies (e.g. to transitioning team, owning unit, or authorized personnel).

Before logging into e-ISuite you must read and agree to the security statement that displays.

PII Data:

PII data is Personally Identifiable Information.

The e-ISuite application limits access to data based on roles assigned to User Accounts. A user can only access data that is relevant to their assigned role.

The e-ISuite database may contain PII data, such as Social Security Numbers (SSN), Tax Identification Numbers (TIN), address and phone information.

The SSN and TIN are encrypted in the database and are never visible to the user in e-ISuite.

All data export files are encrypted for security purposes to protect PII and other sensitive data.