Incident Suite (I-Suite)

Access Control and Account Management Plan

Version 2.2

USDA FOREST SERVICE

Prepared by: FIRE AND AVIATION MANAGEMENT

Date: August 2, 2011

Document Information

Owner Details	
Name	Robert E. Anderson (Acting)
Contact Number	(208) 387-5961
E-mail Address	reanderson@fs.fed.us

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	January 2009	Gina Bald	Original Version
1.1	July 2009	Gina Bald	Updated
2.0	September 2010	Gina Bald	Updated
2.1	November 2010	Gina Bald	Reviewed by Jon Skeels, Robert Anderson. Removed ROB forms.
2.2	August 2011	Gina Bald	Updated, Minor Changes

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
Robert E. Anderson	Acting System Owner	US Forest Service, Fire and Aviation Management	(208) 387-5961
Robert E. Anderson	Information System Security Officer	US Forest Service, Fire and Aviation Management	(208) 387-5961
Jon C. Skeels	Senior Project Manager	US Forest Service, Fire and Aviation Management	(303) 236-0630
Gina Bald	Deputy Project Manager	US Forest Service, Fire and Aviation Management	(801) 531-5325

SIGNATURES

/s/ Robert E. Anderson	07/26/11
Acting System Owner Robert E. Anderson	Date

/s/ Jon C.Skeels	08/01/11
Senior Project Manager Jon C. Skeels	Date

/s/ Robert E. Anderson	07/26/11
Information System Security Officer Robert E. Anderson	Date

Table of Contents

1 INTRODUCTION

This I-Suite Access Control and Account Management Plan (the Plan) details the access control and account management activities for the Incident Suite (I-Suite) application. It facilitates compliance with the National Institute of Standards and Technology's (NIST) *Recommended Security Controls for Federal Information Systems* (NIST 800-53) and the NIST *Guide for Accessing the Security Controls in Federal Information Systems* (NIST 800-53A). Specifically, the following NIST Access Controls (AC) are addressed:

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management
- AC-3 Access Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege

This Plan also relates to three Forest Service SecureCAP procedures:

- *Managing User Accounts for Major Applications*
- *Recertification of User Accounts and Identifying and Establishing Separation of Duties*
- *Maintaining Least Privilege for Users*

1.1 PURPOSE AND SCOPE

The purpose of this Plan is to inform the interagency user community and its leadership about I-Suite access control and account management requirements, processes, guidelines, and user account review and recertification procedures. All I-Suite users should review this Plan to familiarize themselves with it. The Plan is posted on the I-Suite Website (http://isuite.nwcg.gov/) under 'Document Library.' Implementation of the requirements set forth is mandatory.

The scope of this Plan is limited to access control and account management requirements for the I-Suite application. The I-Suite application is defined as the production application used to conduct incident management activities. These security requirements only apply to the production instance of the I-Suite application.

The scope of this Plan does not include the I-Suite system nor does it include the National Data Repository (NDR) host system or the Fire National Enterprise Support System (Fire NESS), which serves as the General Support System (GSS) for the NDR. Fire NESS is hosted at the USDA National Information Technology Center (NITC). Physical and technical access controls to the I-Suite system and for the Fire NESS system are addressed separately.

1.2 ACCESS CONTROL AND ACCOUNT MANAGEMENT FOR I-SUITE

1.2.1 ABOUT I-SUITE

I-Suite is an interagency application with users in the US Forest Service, Department of Interior (DOI) National Park Service (NPS), Bureau of Land Management (BLM), Fish and Wildlife Service (FWS), and Bureau of Indian Affairs (BIA), Department of Homeland Security – Federal Emergency Management Administration (DHS-FEMA), State Forestry Agencies (50 states) and Municipal agencies.

I-Suite allows users to provide automated information management and tracking support for key incident business management functions. Some users access I-Suite regularly throughout the year, while others may use I-Suite once or twice a year.

I-Suite is presently a local network or client application downloaded from the I-Suite website (http://isuite.nwcg.gov/index.html) and installed primarily on computer workstations deployed at incident locations. I-Suite is a single application integrating functional modules and a local database installed on both desktop and laptop computers supporting a host agency unit or an Incident Command Post (ICP) and the outlying areas attached to the ICP.

1.2.2 I-SUITE'S UNIQUE BUSINESS NEEDS

Since I-Suite must support its interagency user community, many components of the Access Control and Account Management procedures set forth in the Forest Service SecureCAP documentation are not feasible for implementation in I-Suite (e.g., initiating a Forest Service Helpdesk ticket to initiate a user account request is not possible for the interagency I-Suite user community).

As a result, the I-Suite team has developed this Plan to support Access Control and Account Management for the I-Suite application. The Plan reflects the need to manage I-Suite application user accounts in a decentralized environment.

For more information about security compliance requirements see Appendix A, "NIST 800-53A Audit Checklist."

1.3 ROLES AND RESPONSIBILITIES

For the purposes of auditing, the roles and responsibilities are divided into two focus areas:

- Security Governance – which focuses on those responsible for maintaining the I-Suite Access Control and Account Management Plan (e.g., ensuring that it is up-to-date, ensuring that it meets the NIST requirements)
- Security Implementation – which focuses on those responsible for implementing the requirements set forth in the I-Suite Access Control and Account Management Plan throughout the broader user community

1.3.1 SECURITY GOVERNANCE

Security governance responsibilities are a critical component of this Plan. There are three roles responsible for security governance:

- System Owner (SO)
- Senior Project Manager (PM)/Deputy Project Manager(DPM)
- Information System Security Officer (ISSO)

1.3.1.1 SYSTEM OWNER

The SO is the approval authority for this Plan and approval. The SO's approval signifies concurrence with the requirements and demonstrates management's commitment to the security requirements outlined in this Plan. The SO is responsible for the annual review of this Plan in accordance with the SecureCAP procedure, "Identifying and Establishing Separation of Duties and Maintaining Least Privilege for Users."

1.3.1.2 SENIOR PROJECT MANAGER AND DEPUTY PROJECT MANAGER

The I-Suite Senior PM and/or DPM are responsible for the following:

- Maintaining and updating this Plan and associated documents
- Requesting SO and ISSO reviews of this plan as necessary
- Maintaining, updating, and administering the requirements of this Plan
- Communicating the requirements of this plan to the Computer Technical Specialist (CTSP)/System Administrator (SA) community

1.3.1.3 INFORMATION SYSTEM SECURITY OFFICER

The ISSO works in collaboration with the Project Manager(s) in the administration of this Plan. The ISSO has key responsibilities for implementation of the security requirements. The ISSO, in conjunction with the SO, is responsible for the following:

- Reviewing this Plan annually in accordance with the SecureCAP procedure, "Identifying and Establishing Separation of Duties and Maintaining Least Privilege for Users."

1.3.2 SECURITY IMPLEMENTATION

Security implementation responsibilities focus on implementing the access controls and account management processes outlined in this Plan. The following positions are responsible for security implementation:

- PM/DPM
- ISSO
- CTSP/SA
- Privileged User
- Basic User

1.3.2.1 PM/DPM AND ISSO

The PM/DPM and ISSO are responsible for the following:

- Communicating the requirements of this plan to the CTSP/SA community
- Providing guidance/training at the CTSP forum on the requirements of this plan
- Assisting the CTSP community with any implementation challenges

1.3.2.2 COMPUTER TECHNICAL SPECIALIST /SYSTEM ADMINISTRATOR

The CTSP/SA is often the same person at an incident. This position is responsible for the following:

- Implementing the security requirements outlined in this Plan
- Ensuring compliance with I-Suite application security requirements within the incident or local unit including:
    - Managing access control requests to I-Suite at each incident or for a local unit, including assigning module access for each access role
    - Establishing and maintaining an environment where computer security, both physical and logical, is a high priority
    - Implementing account review and recertification procedures as defined in Section 3 of this Plan
    - Conducting audits of all user accounts and access rights
    - Documenting and upward reporting all audit results

1.3.2.3 PRIVILEGED USER

I-Suite Privileged Users include the CTSP/SA. In addition, the Database Administrator (DB Admin) is a privileged role with responsibilities for assigning user accounts and privileges to users within the I-Suite application. Privileged users are responsible for the following:

- Complying with all the security requirements outlined in this Plan for privileged users
- Electronically accepting the Rules of Behavior document FS 6600-8, "Statement of Information Security Responsibilities for Users with Privileged Access to Information Systems" (See Appendix D)
- Successfully completing their agency's current security awareness training
- Granting access rights to I-Suite users only for their specific incident database and commensurate with the user's duties

1.3.2.4 BASIC USER

Every Basic User is responsible for the following:

- Complying with all the security requirements outlined in this Plan for basic users
- Electronically accepting the Rules of Behavior document FS 6600-7, "Statement of Employee Information Security Responsibilities" for Forest Service employees or FS 6600-6 "Statement of Information Security Responsibilities for Associate Users of Forest Service Systems" if they are a non-Forest Service employee, including Administratively Determined (AD) (See Appendix D)
- Successfully completing their agency's current security awareness training
- If an AD employee, successfully completing security awareness training provided at the incident or local unit.

2 ACCESS CONTROL REQUIREMENTS

All access control requirements are commensurate with the user's duties at a particular incident. For I-Suite, access control is implemented in accordance with the following principles:

- Access Enforcement
- Least Privilege
- Separation of Duties

2.1 ACCESS ENFORCEMENT

Automated Rules of Behavior (ROB) are implemented in I-Suite. There are three different ROBs:

1. Privileged: Users with DB Admin role
2. Forest Service: Users without DB Admin role who are Forest Service employees
3. Non-Forest Service: Users without DB Admin role who are not Forest Service employees. This includes AD employees.

Privileged Users will be presented the ROB for Users with Privileged Access to Information Systems. Non-Privileged Users are required to select the appropriate ROB at first login per database prior to receiving access to the application. If a user elects to decline the ROB, access to I-Suite will not be granted.

In addition, agency security awareness training must be renewed annually by all Federal Agency users in accordance with their Agency policy. Other I-Suite access enforcement features are provided by the application, which includes:

- Password syntax and character set rules
- One User ID/password combination per user
- Passwords that expire every 60 days
- Password history
- Locked user accounts after five consecutive failed login attempts

2.1.1 PASSWORD SYNTAX AND CHARACTER SET RULES

I-Suite passwords must be between 12 to 31 characters in length and may consist of upper or lower case letters, numbers, and/or special characters as follows:

- minimum of one capital letter
- minimum of one lower case letter
- minimum of one number
- minimum of one special character (!#%^&*_)

The password set by the CTSP/SA is used the first time the user logs on to I-Suite. Once logged on, the user must create and confirm a new password following the syntax and character set rules.

2.1.2 ONE USER ID/PASSWORD COMBINATION PER USER

Every I-Suite user ID must be unique (See Appendices E and G) and will have one corresponding password.

2.1.3 PASSWORDS THAT EXPIRE EVERY 60 DAYS

I-Suite passwords expire every 60 days.

2.1.4 PASSWORD HISTORY

A password history identifies the previous twenty-four passwords used by each I-Suite Application User. A password can be reused after a minimum of twenty-four different passwords.

2.1.5 LOCKED ACCOUNTS AFTER FIVE CONSECUTIVE FAILED LOGON ATTEMPTS

The user must contact the CTSP/SA in the event of a locked user account so that the password may be reset.

2.2 LEAST PRIVILEGE

The CTSP/SA must grant only those access rights required to perform the job. No access rights are granted that are not directly related to the user's official duties. This "least privilege" mitigates the risk for incident management operations. Users may only access those screens and perform only their assigned functions. *See Appendix H., Least Privilege and Separation of Duties Tables for verification information.*

2.3 SEPARATION OF DUTIES

The I-Suite application incorporates appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Users within the I-Suite Application are granted rights that provide them with the level of access required to do the work. *See Appendix H., Least Privilege and Separation of Duties Tables for verification information.*

2.3.1 DATABASE ADMINISTRATOR

The Database Administrator (DB Admin) access right is a privileged user account assigned by the CTSP/SA. Only the DB Admin right may access the "User Management" screen, which allows the DB Admin to set up and manage a user account, designate one or more user rights for that user account based on "least privilege" at the current incident or local unit, and designate an initial password.

Application rights are most often divided among different individuals on an incident or local unit. There are cases, however, where due to the number of employees on an incident or local unit, a user may need many rights. On smaller incidents, a person with the DB Admin right may also require another right, such as Time or Resources. In this case, the user has two user accounts to allow for separation of duties:

- One user account has the DB Admin access right assigned
- One user account has all other appropriate access rights assigned

User Accounts assigned by the System Administrator with DB Admin access rights are "privileged." Privileged accounts can only have access to DB Admin and the Data Admin modules. DB Admin access rights allow the following: User Management, Import/Export of data, Purging SSN/EIN, and Attach/Detach, Rename, Backup, Restore, Copy, Merge, Auditing, and Create new databases within the I-Suite application. Other module access will require a separate account.

2.3.2 BASIC USER

The Basic User may have many assigned access rights except the DB Admin access right. The Basic User can create, edit, and delete incident resource information and create reports.

3 USER ACCOUNT REVIEW AND RECERTIFICATION

The review and recertification of user accounts is conducted at least once during an incident assignment and annually in a local unit setting by the CTSP/SA.

3.1 COMPUTER TECHNICAL SPECIALIST/ SYSTEM ADMINISTRATOR REVIEW TASKS

To complete the review, the CTSP/SA must assess and manage user accounts within their incident assignment or local unit. The CTSP/SA will review all (100 percent) of I-Suite users within their incident assignment or local unit. The CTSP/SA then completes the Review and Recertification Report (Appendix F.) by performing the following tasks:

- Deactivate inactive user accounts that have not reset the initial password within 3 days of creation
- Deactivate duplicate user accounts
- Verify that least privilege is assigned to user accounts
- Ensure separation of duties for Basic user accounts
- Ensure separation of duties for Database Administrator user accounts
- Submit review logs to the ISSO

For more information on Review tasks, see Appendix B, "Review Procedures"

All CTSPs/SAs are responsible for taking the corrective actions necessary to make compliant the user accounts under their review.

3.2 AUDIT METHODOLOGY

The CTSP/SA will conduct an audit at least once during an incident assignment and annually in a local unit setting. The Auditing function is accessed by user accounts with the DB Admin access right. Auditing allows users to audit the following activities within the I-Suite application:

- I-Suite Login History – Logins and Logoffs of different databases

- External Access History – External User Accounts that have accessed an I-Suite database in an external application
- User Account History – Changes made to User and Admin Accounts
- External Account History – Changes made to External User Accounts

The CTSP/SA will also confirm the following:

- Least privilege for all user accounts has been verified
- Separation of duties for all user accounts has been verified

See Appendix H., Least Privilege and Separation of Duties Tables for verification information.

3.3 REPORTING AUDIT RESULTS

The CTSP/SA is responsible for completing and signing the Review and Recertification Report (Appendix F.) and retaining hard copies at their incident or local unit as appropriate. *For detailed review procedures see Appendix B, "Review Procedures."*

In addition to the audit performed by the CTSP/SA, the I-Suite Senior Project Manager or designee may conduct spot check audits during incident or local unit visits. Spot check audit results are maintained by the auditor and also submitted to and retained by the CTSP/SA. The signed documents will be filed in the incident documentation package and turned over to the host agency. The local unit will maintain those records for the period of time as stated in FSH 6209.11, Chapter 40. *See Appendix C, I-Suite Incident Checklist for audit items.*

In the event that an audit finding results in the identification of a security "incident', reports of findings will be submitted to the ISSO and Incident Commander or Agency Administrator for corrective action.

3.4 IMPLEMENTATION

Formal implementation of this Access Control and Account Management Plan shall be carried out by all CTSP/SA and I-Suite application users.

3.4.1 CONSEQUENCES FOR FAILURE TO COMPLY

Failure to comply with the requirements set forth in this Plan has consequences, depending on the severity of the infraction. Consequences for failure to comply are described in the Rules of Behavior. In addition, any indication that account management activities are being conducted improperly at an incident or local unit will result in an audit of all accounts within that incident or local unit by the I-Suite Project Team or ISSO. Should findings reveal that account management activities are not conducted in accordance with the requirements, a letter will be sent to the Incident Commander, Unit Manager, and/or Agency Manager. Further action may also be taken.

For a copy of the Rules of Behavior see, Appendix D, "Rules of Behavior Requirements and Forms."

Appendix A: NIST 800-53A Audit Checklist

This audit checklist facilitates compliance with the following federal requirements, including the National Institute of Standards and Technology's (NIST) *Recommended Security Controls for Federal Information Systems* (NIST 800-53) and the NIST *Guide for Accessing the Security Controls in Federal Information Systems* (NIST 800-53A). These two documents outline the following NIST Access Controls (AC):

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management
- AC-3 Access Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege

NIST Control	Description	Document(s) Where Addressed
AC-1.1	The organization develops and documents access control policy and procedures	I-Suite Access Control and Account Management Plan
AC-1.1	The organization disseminates access control policy and procedures to appropriate elements within the organization.	The I-Suite Access Control and Account Management Plan to the Computer Technical Specialist (CTSP) Taskgroup, identified System Administrators (SA), and posted to the I-Suite web site.
AC-1.1	Responsible parties within the organization periodically review access control policies and procedures	Section 1.3.1, "Security Governance outlines the roles and responsibilities of the SO, Sr. Project Manager/Deputy Project Manager, and ISSO.
AC-1.1	The organization updates access control policy and procedures when organizational review indicates updates are required	Section 1.3.1, "Security Governance," outlines policy and procedure update and review by the SO, Sr. Project Manager/Deputy Project Manager, and ISSO.
AC-1.2	The access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance	The I-Suite Access Control and Account Management Plan outlines the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.
AC-1.2	The Access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.	Section 1.2, "Access Control and Account Management for I-Suite," describes the mission and business needs that I-Suite meets and Section 1 identifies the NIST 800-53 Access Controls addressed in this Plan.
AC-1.2	The access control procedures address all areas identified in the access control policy and address achieving policy compliant implementations of all associated security controls.	This Plan addresses key NIST Access Control requirements and focuses on achieving policy compliance.
AC-2(1).1	The organization employs automated mechanisms to support information system account management functions.	Automated Rules of Behaviors are implemented in I-Suite.
AC-2(1).2	The organization system automatically terminates temporary and emergency	N/A. No temporary or emergency accounts are allowed in I-Suite.

NIST Control	Description	Document(s) Where Addressed
	accounts.	
AC-2(2).1	The organization defines a time period after which the information system terminates temporary and emergency accounts.	N/A. No temporary or emergency accounts are allowed in I-Suite.
AC-2(2).1	The system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.	N/A. No temporary or emergency accounts are allowed in I-Suite.
AC-2(3).1	The organization defines a time period after which the information system disables inactive accounts	User accounts are deactivated. Section 3.1, "Deactivate inactive user accounts," outlines the 3-day inactivity timeframe before a user account becomes deactivated.
AC-2(3).1	The system automatically disables inactive accounts after organization-defined time period	User accounts are deactivated by the CTSP/SA. Section 3.1, "Deactivate inactive user accounts," outlines the 3-day inactivity timeframe before a user account becomes deactivated.
AC-2(4).1	The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions	Section 2.3, "Separation of Duties," details the Database Administrator access right, which is the only access right that may create, modify, or deactivate a user account. Auditing procedures are described in Section 3.2.
AC-2(4).1	The organization employs automated mechanisms to notify, as required, appropriate individuals.	Section 3.1, "System Administrator Review Tasks," outlines the process and details the completion of the Review and Recertification Report.
AC-3.1	The system enforces assigned authorizations for controlling access to the system in accordance with applicable policy	Section 2.1, "Access Enforcement," outlines access enforcement features to control access to I-Suite.
AC-3.1	User privileges on the system are consistent with the documented user authorizations	Section 2.2, "Least Privilege," outlines CTSP/SA responsibilities for granting access rights.
AC-3(1).1	The organization explicitly defines privileged functions and security-relevant information for the system.	The CTSP/SA is responsible for all privileged user access to I-Suite.
AC-3(1).1	The organization explicitly authorizes personnel access to privileged functions and security-relevant information	The CTSP/SA is responsible for all personnel access to I-Suite. Section 2.2, "Least Privilege," outlines the responsibilities for controlling access.
AC-3(1).1	The system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel	The CTSP/SA is responsible for all privileged user access to I-Suite. Hardware is outside the boundary of I-Suite.
AC-5.1	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflict of interest in the responsibilities and duties of individuals	Section 2.3, "Separation of Duties," defines the separation of duties between the Database Administrator access right and all other access rights in I-Suite.
AC-5.1	The system enforces separation of duties	Section 2.3, "Separation of Duties identifies the

NIST Control	Description	Document(s) Where Addressed
	through assigned access authorization	Database Administrator access right as the only access right that cannot be combined with other access rights.
AC-6.1	The organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks	Section 2.3, “Separation of Duties identifies the Database Administrator access right as the only access right that cannot be combined with other access rights.
AC-6.1	The information system enforces the most restrictive set of rights/privileges or access needed by users	Section 2.2, “Least Privilege,” outlines CTSP/SA responsibilities to ensure least privilege.

APPENDIX B. REVIEW PROCEDURES

This appendix provides the I-Suite CTSP/SA with a procedure for reviewing I-Suite user accounts and access rights to complete the "Review and Recertification Report" (Appendix F.)

Scope

This procedure applies to all I-Suite basic and privileged user accounts for the I-Suite application. The I-Suite application is categorized as a moderate system according to the Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems.*

Prerequisites and Tools

1. Trigger: When there is a significant increase or decrease of 25% or more in I-Suite users.
2. Trigger: When I-Suite user accounts are reviewed by the I-Suite CTSP/SA
3. Prerequisite: Completion of the User Account Review Checklist
4. Prerequisite: Completion of the Privileged User Account Review Checklist
5. Prerequisite: Completion of the Review and Recertification Report
6. Tool: Access Control and Account Management Plan

Procedures

□ **1 Conduct I-Suite user account recertification and audit.**

□ 1.1 No less than once on an incident, annually in a local unit or otherwise specified in the System Security Plan, the I-Suite CTSP/SA:

□ 1.1.1 Obtains and reviews all I-Suite user accounts within their incident or local unit.

□ 1.1.1.1 Identifies, by working with appropriate Supervisor(s) those person(s) with I-Suite user accounts who should be deactivated due to demobilization or no longer needing access.

□ 1.1.1.2 Identifies I-Suite user accounts that have not reset the initial password within three days of creation.

□ 1.1.1.3 Identifies those persons with duplicate I-Suite user accounts by reviewing the User Management screen.

- 1.1.1.4 Verifies that the least privilege is assigned to I-Suite user accounts.

- 1.1.1.5 Ensures separation of duties for I-Suite Database Administrator user accounts.

- 1.1.2 Documents review results for least privilege and separation of duties on the User Account Review Checklist.

- 1.1.3 Documents review results for privileged user accounts on the Privileged User Account Review Checklist.

- 1.1.4 Compiles and completes review results on the Review and Recertification Report.

- 1.1.5 Signs the Review and Recertification Report and submits it to the Information System Security Officer (ISSO).

- 1.2 The CTSP/SA retains the Review and Recertification Report to support any IT security investigations and/or incidents. The signed documents will be filed in the incident documentation package and turned over to the host agency. The local unit will maintain those records for the period of time as stated in FSH 6209.11, Chapter 40.

- **2 Stop I-Suite user account recertification and audit.**

Resulting Documentation

1. Completed Review and Recertification Report.

Reporting Problems

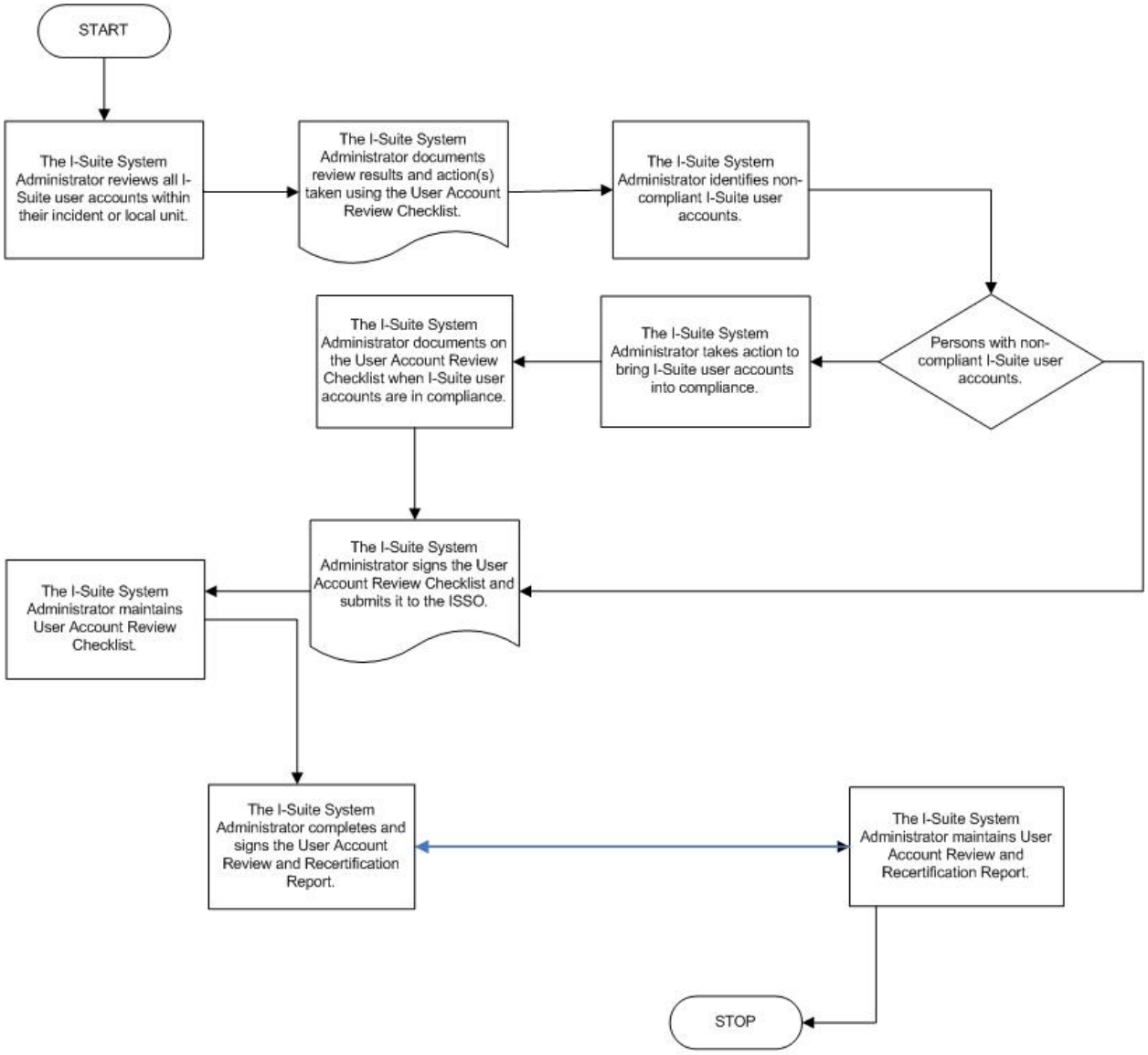
When anomalies or problems arise in the completion of this procedure that cannot be resolved, the CTSP/SA will report them to the I-Suite ISSO.

Related Procedures

1. Section 3, "User Account Review and Recertification."

2. "Information Technology Procedures AU-6/AC-13 Audit Review." [Online]. Available http://fsweb.wo.fs.fed.us/ftp/pub/open/cio/SecureCAP.

Process Diagram



APPENDIX C. I-SUITE INCIDENT CHECKLIST

I-Suite Incident Checklist

Incident Number:_____Incident Name:_____

IMT:_____CTSP: _____

The following items were spot checked during the incident visit:

Item	Yes	No	Remarks
Backups Performed			
Backup Screenshot			
Backups Saved to External Location			
User Accounts/ Naming Conventions			
External Accounts (EA)			
Separation of Duties			
Least Privilege			
Audit Logs Reviewed			
Incident User Acceptance Forms			

Checklist completed by:_____.
Name Title

APPENDIX D. RULES OF BEHAVIOR REQUIREMENTS AND FORMS

Automated Rules of Behavior (ROB) are implemented in I-Suite. There are three different ROBs:

1. Privileged: Users with DB Admin right
2. Forest Service: Users without DB Admin right who are Forest Service employees
3. Non-Forest Service: Users without DB Admin right who are not Forest Service employees. This includes AD employees.

Privileged Users will be presented the ROB for Users with Privileged Access to Information Systems. Non-Privileged Users are required to select the appropriate ROB at first login per database prior to receiving access to the application. If a user elects to decline the ROB, access to I-Suite will not be granted.

Logging In

Automated "Rules of Behavior":

- Privileged User
- Forest Service User
- Non- Forest Service User (Including AD's)

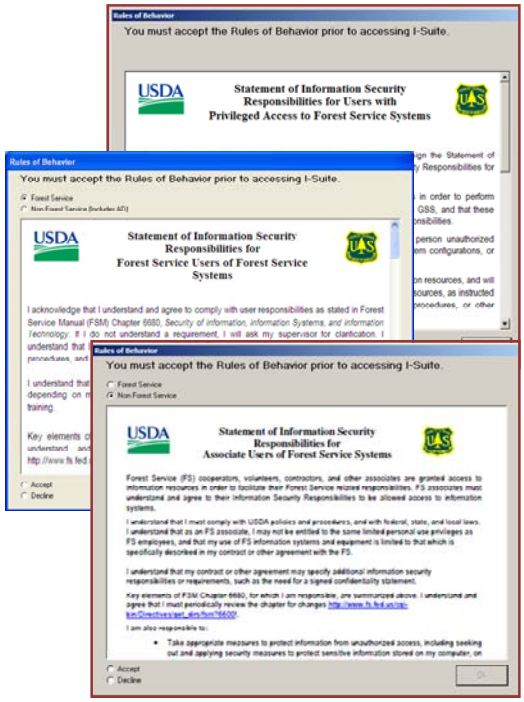


Exhibit 01 Rules of Behavior Screenshot

The following Rules of Behavior apply when to creating an I-Suite user account:

- 6600-6: Statement of Information Security Responsibilities for Associate Users of Forest Service Systems
- 6600-7: Statement of Employee Information Security Responsibilities

- 6600-8: Statement of Information Security Responsibility for Users with Privileged Access to Information Systems

Table 1, "Rules of Behavior Requirements for I-Suite Users" outlines the required Rules of Behavior by type of user.

Type of Account and Employment Status	Rules of Behavior Version Number		
	6600-6	6600-7	6600-8
System Administrator			
Forest Service Employees			X
Federal Agency (non-FS) Employees			X
State Employees			X
Emergency Hires (AD)			X
I-Suite Privilege Users			
Forest Service Employees			X
Federal Agency (non-FS) Employees			X
State Employees			X
Emergency Hires (AD)			X
Contract Employees			X
I-Suite Basic Users			
Forest Service Employees		X	
Federal Agency (non-FS) Employees	X		
State Employees	X		
Emergency Hires (AD)	X		
Contract Employees	X		

Table 1: Rules of Behavior Requirements for I-Suite Users

APPENDIX E. USER ACCOUNT NAMING CONVENTIONS

Each user at an incident or local unit must have a unique user account to log in to I-Suite. This improves I-Suite security by limiting access to just that individual and promotes individual accountability. The current naming conventions for assigning a user account include:

- all lower case letters
- first initial, last name
- two digit, sequential number for user accounts with the same first initial and last name.

When assigning a user account to a user, I-Suite will notify you if that user account already exists with an Active status. The existing user must be deactivated before saving the new user as Active. If it is necessary to assign an account with the same username, add the next sequential, two-digit number to the end of the user account name.

Table 2 lists sample naming conventions for the name, "John Smith." Notice that the naming convention is independent of the user's work location.

First Name	Last Name	User Right	Resulting User Account Name
John	Smith	Resources	jsmith
John	Smith	Time	jsmith01
John	Smith	Injury/Illness	jsmith02

Table 2: Naming Conventions

APPENDIX F. USER ACCOUNT REVIEW AND RECERTIFICATION REPORT

User Account Review Checklist

This is a listing of all user accounts within a specified Incident or Local Unit. It is designed to assist the System Administrator in auditing individual user accounts within their responsibility. The form may be printed out and completed by hand or completed online.

Reviewer Information:

Last Name	First Name	Position Title	Report Date

Incident or Local Unit Information

Last Name	First Name	User Account	Function	Least Privilege	Separation of Duties	Change to User Account
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No
				Yes/No	Yes/No	Yes/No

Privileged User Account Review Checklist

This is a listing of all user accounts with privileged access within the I-Suite application at a specified Incident or Local Unit. It is designed to assist the System Administrator in auditing individual user accounts within their responsibility. The form may be printed out and completed by hand or completed online.

Reviewer's Information

Last Name _____ First Name _____ Position Title _____ Report Date _____

Incident or Local Unit Information

Last Name	First Name	User Account	When Created	Right(s) Assigned

Review and Recertification Report

This is an online form submitted by the System Administrator to the ISSO.

Incident or Local Unit: _____Completion Date of Audit:_____

I certify that the I-Suite user accounts for the Incident or Local Unit named have been reviewed and recertified. A copy of this Review and Recertification Report has been submitted to the ISSO and retained at the Incident or Local Unit.

Last Name First Name Position Title

_____ _____ _____

Local Unit Organization Information:

Unit ID Office/Organization Name

_____ _____

Mailing Address State/Province Country/Territory Postal Code

_____ _____ _____

Incident Information:

IMT Name Incident Location

_____ _____

Review Task	Completed (Yes/No)
User accounts were reviewed and deactivated for users who have been released.	Yes/No
User accounts were reviewed and inactivated for user accounts with no activity within the past 3 days.	Yes/No
User accounts were reviewed for multiple occurrences. Any such user accounts have been deactivated.	Yes/No
User accounts were reviewed and access rights were confirmed for "Least Privilege." Access rights were removed/added accordingly.	Yes/No
User accounts were reviewed and access roles were confirmed for "Separation of Duties." Access rights were removed/added accordingly.	Yes/No

APPENDIX G. ACCOUNT ADMINISTRATION

This appendix outlines your responsibility as I-Suite System Administrator to ensure the security of the I-Suite application by preventing/reducing the likelihood of unauthorized or inappropriate access. It outlines guidelines and step-by-step instructions to set up user accounts and assign access rights to I-Suite users within your incident or local unit. This guide also explains the tasks necessary to review and recertify user accounts and access rights. Before proceeding, be sure you are familiar with the following topics:

- Understanding I-Suite user accounts and access rights
- Ensuring security compliance for each I-Suite user

UNDERSTANDING I-SUITE USER ACCOUNTS AND ACCESS RIGHTS

As a System Administrator, you are responsible for determining, assigning, and maintaining user accounts and appropriate access rights for all I-Suite users on your incident or in your local unit. Terminology employed in this guide includes the following:

- I-Suite Users
- User Accounts
- Passwords
- Rights

I-SUITE USERS

An I-Suite user is anyone who has an I-Suite user account and can log into and access the I-Suite application. Automated Rules of Behavior (ROB) are implemented in I-Suite. There are three different ROBs:

1. Privileged: Users with DB Admin role
2. Forest Service: Users without DB Admin role who are Forest Service employees
3. Non-Forest Service: Users without DB Admin role who are not Forest Service employees. This includes AD employees.

Privileged Users will be presented the ROB for Users with Privileged Access to Information Systems. Non-Privileged Users are required to select the appropriate ROB at first login per database prior to receiving access to the application. If a user elects to decline the ROB, access to I-Suite will not be granted.

In addition, agency security awareness training must be renewed annually by all Federal Agency users in accordance with their Agency policy.

> *For more information about the Rules of Behavior agreement see Appendix D, "Rules of Behavior Requirements and Forms."*

USER ACCOUNTS

In I-Suite, a user account is the login ID of the I-Suite user. Every user account identifies the user's name, the type of access, and the assigned rights. There is a one-to-one relationship between the user account and its password.

A user account with the Database Administrator right assigned to it may not have more than one assigned access right, based on what the user requires to perform the job. This is called "Least Privilege." A user account with the Database Administrator right assigned to it may not have any other assigned access rights. This is called "Separation of Duties." As a System Administrator, you must ensure that user accounts within the incident or local unit comply with the rules associated with least privilege and separation of duties.

For more information about least privilege and separation of duties refer to Section 2.2, "Least Privilege," and Section 2.3, "Separation of Duties and see Appendix H. I-Suite Least Privilege and Separation of Duties Tables.

USER PASSWORDS

A password has a one-to-one relationship with a user account. When you first create a user account you will also assign an initial password. The password must be changed the first time the user logs on to I-Suite. The new password must be between 12 to 31 characters in length and must consist of upper or lower case letters, numbers, and/or special characters.

ACCESS RIGHTS

In I-Suite, an access right defines the modules a user may access. The Database Administrator user account has "privileged" access rights. The following restrictions apply to access rights:

Database Administrator - May not have any other assigned access rights(s).
Basic User Accounts - These non-Database Administrator user accounts may have more than one assigned access right.

MANAGING USER ACCOUNTS

The System Administrator is responsible for managing user accounts within their incident or local unit.

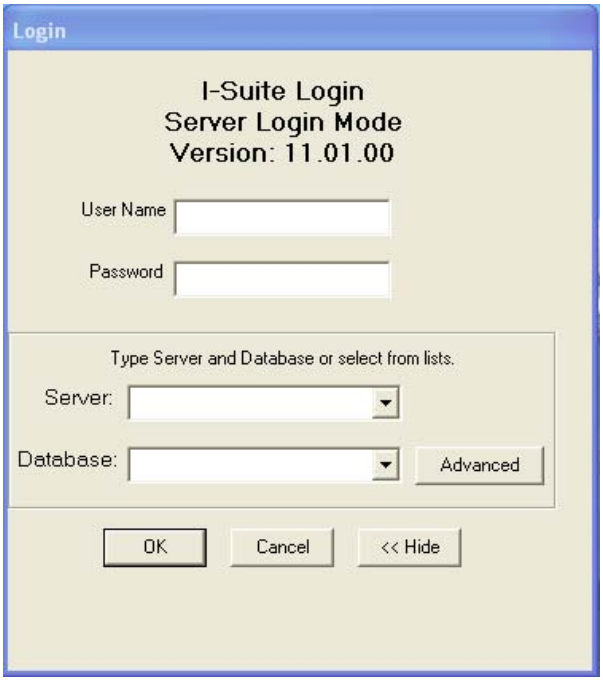
The following topics outline System Administrator tasks for managing user accounts:

- Logging into I-Suite
- Creating a user account and assigning access rights
- Activating a user account
- Deactivating a user account
- Assigning/Removing access rights
- Changing a user account password
- Resetting a user account password

Refer back to these tasks when reviewing/recertifying user accounts

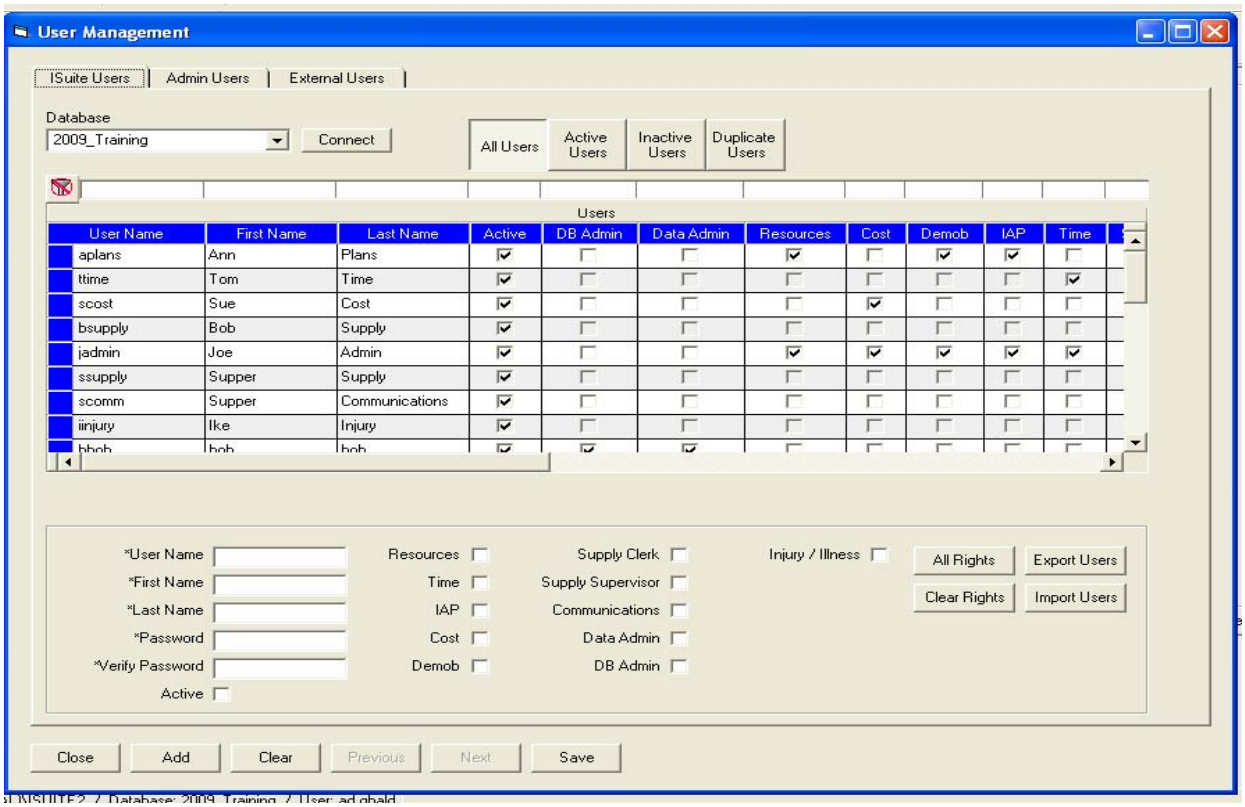
To log into I-Suite and display the User Management screen

1. From the **Desktop**, double-click the **I-Suite** icon.
2. On the **WARNING** dialog box, click **Yes**.
3. On the **Login** dialog box, type your **DB Admin User Name**, press TAB, type your **DB Admin Password**, **Server**, and **Database**. Click **OK**.



4. From the **Modules** drop-down menu, select the **Database Admin** option to open the **Database Admin** window.

5. Click the **Users** button to display the **User Management** window.



6. Click the **ISuite Users** tab to select it.

7. Click the **Add** button to add a new user.

8. Enter the **User Name** the person must enter to log into the I-Suite system.

9. Enter the person's **First Name** and **Last Name**.

10. Enter the **Password** the person must enter to log into the I-Suite system for the first time. Once the user logs on to I-Suite the first time, the password must be changed.

11. In the **Verify Password** box, re-enter the password to make sure it was entered correctly.

12. Click to check one or more of the following rights. When you check an option, the user can access that particular module or function in the I-Suite system:

    - Resources
    - Time
    - IAP
    - Cost
    - Demob

- Supply Clerk
- Supply Supervisor
- Communications
- Data Admin
- DB Admin
- Injury/Illness

13. To assign all rights to the I-Suite user, click the **All Rights** button. The **All Rights** button assigns all rights to a user, except **Injury/Illness** rights. You must click the **Injury/Illness** checkbox to assign those rights to a user.

14. To remove all rights from the I-Suite user, click the **Clear Rights** button.

15. To activate the I-Suite user, click to check the **Active** checkbox.

16. To save your changes, click the **Save** button.

If the account already exists, the following message will appear:

17. When the **Data Saved** message displays, click the **OK** button.

18. To close the **User Management** window, click the **Close** button.

Deactivating an I-Suite User

1. From the **Modules** drop-down menu, select the **Database Admin** option to open the **Database Admin** window.

2. Click the **Users** button to open the **User Management** window.

3. Click the **ISuite Users** tab to select it.

4. Under **Users**, click to select the appropriate user name.

5. Click to uncheck the **Active** checkbox.

6. To save your changes, click the **Save** button.

7. When the **Data Saved** window displays, click the **OK** button to close the window.

8. To close the **User Management** window, click the **Close** button.

Changing Access Rights for an I-Suite User

Users only have access to the various modules and functional areas of I-Suite that have been checked on the ISuite Users window.

1. From the **Modules** drop-down menu, select the **Database Admin** option to open the **Database Admin** window.

2. Click the **Users** button to open the **User Management** window.

3. Click the **ISuite Users** tab to select it.

4. Under **Users**, click to select the appropriate user name.

3. Click to check or uncheck the following checkboxes to assign the appropriate rights to the user. Checking one of the following boxes gives the selected I-Suite User permission to access that particular module or functional area in I-Suite. If you uncheck a checkbox, the user can no longer access that area of the I-Suite application:

    - Resources
    - Time
    - IAP
    - Cost
    - Demob
    - Supply Clerk
    - Supply Supervisor
    - Communications
    - Data Admin
    - DB Admin
    - Injury/Illness

5. To save your changes, click the **Save** button.

6. When the **Data Saved** window displays, click the **OK** button to close the window.

7. To close the **User Management** window, click the **Close** button.

Changing User Password

1. From the **Modules** drop-down menu, select the **Database Admin** option to open the **Database Admin** window.

2.Click the **Users** button to open the **User Management** window.

3.Click the **I-Suite Users** tab to select it.

4.Under **Users**, click to select the appropriate **User Name**.

5.In the **Password** box, enter a temporary password for the user.

6.In the **Verify Password** box, re-enter the password to make sure it was entered correctly.

7. To save your changes, click the **Save** button.

To reset a user account password

The user is automatically locked out after five consecutive failed log-in attempts or after 60 days of user account inactivity

1. From the **Modules** drop-down menu, select the **Database Admin** option to open the **Database Admin** window.

2. Click the **Users** button to open the **User Management** window.

3. Click the **ISuite Users** tab to select it.

4. Under **Users**, click to select the appropriate user name.

5. Click to check the **Active** checkbox.

6. To save your changes, click the **Save** button.

7. When the **Data Saved** window displays, click the **OK** button to close the window.

8. To close the **User Management** window, click the **Close** button.

9. The user will login with their previous password.

APPENDIX H. LEAST PRIVILEGE AND SEPARATION OF DUTIES TABLES

The following Least Privilege table documents the User Roles, Responsibilities, and Permissions/Privileges needed to fulfill job functions for I-Suite.

User Role	User Role Responsibilities	Permissions/Privileges
Database Administrator (DB Admin)	Adds end users; Grants Roles; Access to the I-Suite Server; Attach, Detach, Backup, Restore, Copy, Create, and Rename Database; Import and Export Data; Create Repository; Purge SSN/EIN; Activate/Deactivate Users, Auditing	Read, Write Application Access to Database
Data Admin	Enters incident, accounting code and lookup tables data into the database; Create Custom Reports	Read, Write, Update, and Delete Data
Resources	Enters Resource Data, Creates Canned and Custom Reports	Read, Write, Update, and Delete Data
Time	Enters Resource Data, Creates Canned and Custom Reports; Enters Resource Time and Adjustments Data; Enters Contractor and Administrative Office Data	Read, Write, Update, and Delete Data
IAP	Enters Incident Action Plan Data; Creates Custom Reports	Read, Write, Update, and Delete Forms
Cost	Enters Resource Data, Creates Canned and Custom Reports; Enters Cost Data, Acres Burned, Divisions, and Rates; Creates Accruals, Graphs, and Projections	Read, Write, Update, and Delete Data
Demob	Enters Resource Data, Creates Canned and Custom Reports; Enters Demob Data	Read, Write, Update, and Delete Data
Supply Clerk	Enters Supply Data: Issues, Issue Returns, Receive, Permanent Release, Locations, Supply Items, Transfers; View Supply History; View Inventory; Create Custom and Canned Reports	Read, Write, Update, and Delete Data
Supply Supervisor	Enters Supply Data: Issues, Issue Returns, Receive, Permanent Release, Locations, Supply Items, Transfers; Correct Supply Inventory;	Read, Write, Update, and Delete Data

User Role	User Role Responsibilities	Permissions/Privileges
	View Supply History; Create Custom and Canned Reports	
Communication	Enters Supply Data: Issues, Issue Returns, Receive, Permanent Release, Locations, Supply Items, Transfers; Correct Supply Inventory; View Supply History; Create Custom and Canned Reports	Read, Write, Update, and Delete Data
Injury/Illness	Enters Resource Injury and Illness Data; Creates Custom and Canned Reports; Views History; Creates Statistic Base	Read, Write, Update, and Delete Data

The following Separation of Duties table documents roles which should not be held by a single individual.

	Database Administrator (DB Admin)	Data Admin	Resources	Time	IAP	Cost	Demob	Supply Clerk	Supply Supervisor	Communication	Injury/Illness
CTSP	X					X	X	X	X	X	X
Status Check-In	X			X	X	X		X	X	X	X
Resources Unit Leader	X			X		X		X	X	X	X
Plans Section Chief	X			X		X		X	X	X	X
Demob Unit Leader	X			X	X	X		X	X	X	X
Cost	X				X			X	X	X	X
Time Unit Leader	X				X	X	X	X	X	X	X
Finance Section Chief	X				X		X	X	X	X	X
PTRC	X	X	X		X	X	X	X	X	X	X

	Database Administrator (DB Admin)	Data Admin	Resources	Time	IAP	Cost	Demob	Supply Clerk	Supply Supervisor	Communicatio	Injury/Illness
EQTR	X	X	X		X	X	X	X	X	X	X
Procurement Unit Leader	X				X	X	X	X	X	X	X
Comp/Claims	X	X	X	X	X	X	X	X	X	X	
INJR	X	X	X	X	X	X	X	X	X	X	
Medical Unit Leader	X	X	X	X	X	X	X	X	X	X	
Communications Unit Leader	X	X	X	X		X	X	X	X		X
INCM	X	X	X	X		X	X	X		X	X
Supply Unit Leader	X	X	X	X	X	X	X	X		X	X
RCDM	X	X	X	X	X	X	X	X		X	X
Camp Crew (Supply Clerk)**	X	X	X	X	X	X	X		X	X	X
Database Administrator*			X	X	X	X	X	X	X	X	X

* This is not a position on an Incident. This role can only be used from the I-Suite server machine.

** Supply Clerk is not a position on an Incident. The position is filled with someone from a Camp Crew in most instances; however Other Positions could be used in this function as well.

Users can only access the modules or functions they have been assigned based on their job role. Only authorized users are given administrative usernames and passwords for accessing I-Suite. Assignment of roles is handled by I-Suite System Administrators. For more details, please refer to the I-Suite User's Manual.

The following table documents the roles for I-Suite and the permissions and privileges required for each role to complete its assigned job function.

Role	Permissions and Privileges	Authorized By	**Date**
Database Administrator (DB Admin)	Read, Write Application Access to Database	Authorized at Incident by System Administrator	At Incident
Data Admin	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Resources	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Time	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
IAP	Read, Write, Update, and Delete Forms	Authorized at Incident by System Administrator	At Incident
Cost	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Demob	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Supply Clerk	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident

Role	Permissions and Privileges	Authorized By	**Date**
Supply Supervisor	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Communication	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident
Injury/Illness	Read, Write, Update, and Delete Data	Authorized at Incident by System Administrator	At Incident

Least Privilege Review: Currently, no roles within I-Suite have been assigned permissions or privileges in excess of the least privilege necessary to complete the intended job function.