



## **SUPPLEMENT**

# **I-Suite Rules of Behavior and Separation of Duties**

**THIS SUPPLEMENT IS FOR USE WITH ISUITE V9 TRAINING MANUAL**

3/21/2011

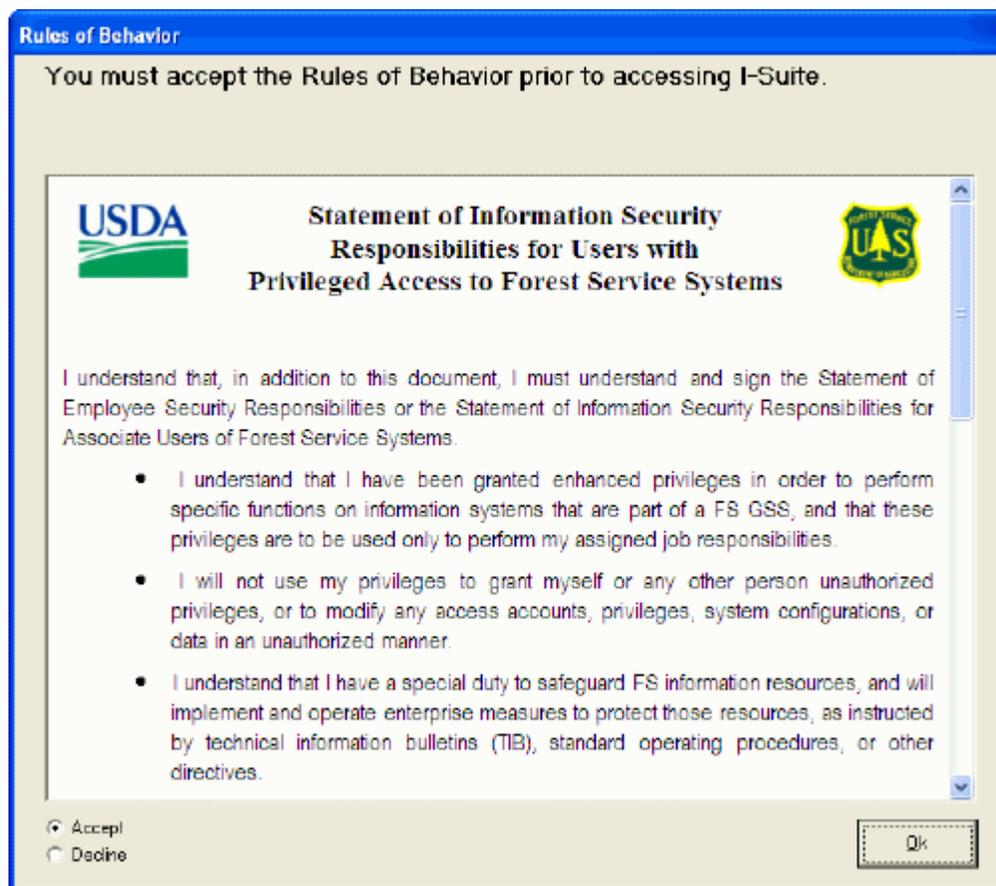
## **Table of Contents**

- 1.0 – Rules of Behavior
- 1.1 – Separation of Duties

## 1.0 RULES OF BEHAVIOR

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

1. The first time an I-Suite user logs in to I-Suite and during the Initial Server Setup process a Rules of Behavior window will be displayed. The user logging in to the system will be required to read and accept the Rules of Behavior before access will be granted to the system. Once a user has accepted the Rules of Behavior, I-Suite will no longer display the Rules of Behavior window during the login process for that user.



2. User must select Accept and click Ok to be granted access to the I-Suite system

**NOTE:** This process applies to every user the first time the user logs in to the application as well as when the Initial Server Setup occurs and the initial Admin user account is created.

## 1.1 SEPARATION OF DUTIES

Separation of DB Admin Duties is now enforced.

- Privileged accounts are restricted to DB Admin and Data Admin module access.
- Other module access will require a separate account.

If a user is set up to have DB Admin privileges they cannot have privileges in other modules except Data Admin. If a user needs DB Admin privileges AND privileges to another module they **MUST** have another user account with the other privileges assigned to that account and the user will be required to use the different accounts depending on the task they intend to perform in I-Suite.