

Rules of Behavior

NATIONAL INTERAGENCY RESOURCE ORDERING AND STATUS SYSTEM (ROSS)

1. Introduction

The following rules of behavior are to be followed by all users of the ROSS. The rules clearly delineate the responsibilities and expectations for all individuals with access to the ROSS. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions taken will be determined by each user's specific agency, with the recommendations of a ROSS security officer or a USDA National Information Technology Center (NITC) security officer or both. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2. Responsibilities

The National Wildfire Coordinating Group's (NWCG) ROSS security officer and the NITC security officer are responsible for ensuring an adequate level of protection is afforded to the ROSS, through an appropriate mix of technical, administrative, and managerial controls. The security officers develop policies and procedures, ensure the development and presentation of user and contractor awareness sessions, and make inspections and spot checks to determine that an adequate level of compliance with security requirements exist. The security officers are responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in the security posture of ROSS. Unit security officers are responsible for all aspects of system security at the unit level. A unit is defined as any specific level of the organization, such as: national, regional, state, or local.

3. Other Policies and Procedures

The rules are not to be used in place of existing agency policy; rather they are intended to enhance and further define the specific rules each user must follow while accessing ROSS.

4. Application Rules

4.1. Working at Home

Agency specific directives, policies, and regulations may designate specific employees (for example: critical job series, employees on maternity leave, and employees with certain medical conditions) as eligible for working at home.

4.2. Dial-up Access

An agency IRM Director may authorize dial-up access to ROSS from locations where network access is not available. It is understood that dial-up access poses additional security risks, but may become necessary to carry out the dispatch job from remote locations, from an employee's home, or from a dispatch office during network outages. If dial-up access is allowed, ROSS and NITC security officers will regularly review telecommunications logs and NITC phone records, and conduct spot-checks to determine if users are complying with controls placed on the use of dial-up lines, and to assure that the proper level of service is provided. All dial-up calls will use username and password pairs that are managed by the National Interagency Coordination Center (NICC). If dial-up access is allowed to other applications on the system on which ROSS resides, the managers of those applications will be notified.

4.3. Software Licenses

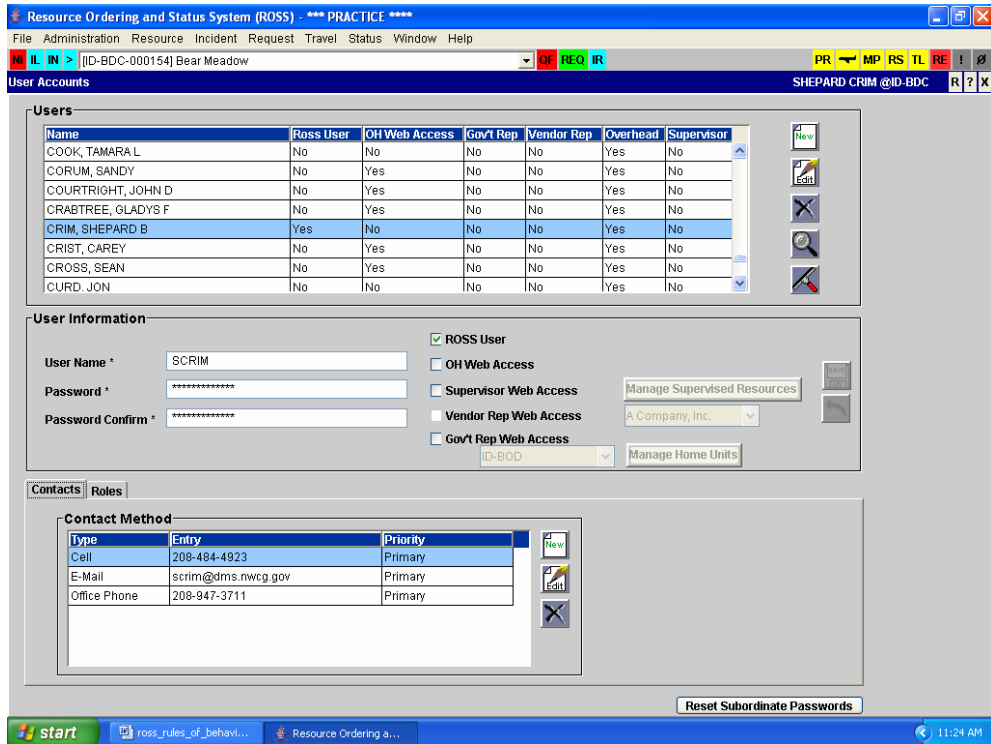
Personnel using ROSS are not required to physically have software licenses. All software licenses associated with the ROSS commercial off-the-shelf (COTS) software are complied with by ROSS. Contractors responsible for developing and maintaining ROSS are also covered by this compliance.

4.4. Unofficial Use of Government Equipment

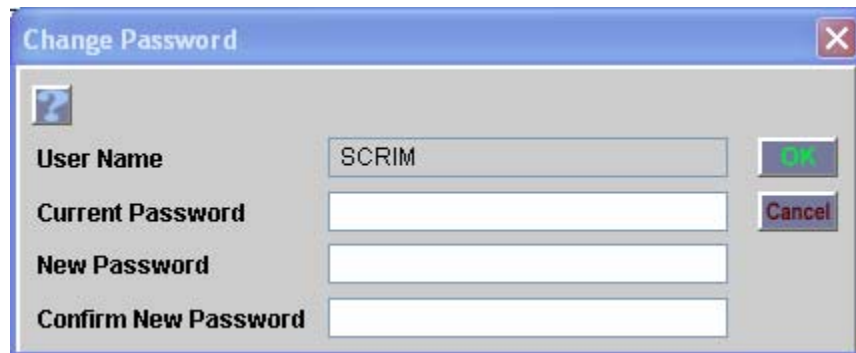
Users should be aware that personal use of information resources is not authorized.

4.5. Use of Passwords

Passwords shall be a combination of at least eight (8) alpha and numeric characters. Users are to keep passwords confidential and are not to share passwords with anyone. Users shall change their passwords every 90 days. User names and passwords are initially created and set by the ROSS Account Manager using the User Accounts screen shown below. Instructions on the proper use of this screen are documented in the ROSS Users Guide and the System Role Descriptions document.



Users can change their passwords by clicking **Change Password** from the **File** menu as depicted below:



4.6. System Privileges

Users are to work within the confines of their authorized access for ROSS and are not to attempt access to application modules or screens to which access has not been authorized.

User accounts and additional roles can be requested through the local ROSS Account Manager.

4.7. Individual Accountability

Users will be held accountable for their actions while using ROSS. Individual accountability is stressed during the ROSS Administration and Dispatch training sessions.

4.8 Virus Checking Software

Agency IRM personnel assure virus checking software is installed and that virus signature files are current for client work stations in accordance with agency policy. Virus checking software must be configured to check all mail attachments. Virus software shall be configured to warn users when an attached message is infected with a virus. When users are warned, appropriate measures shall be taken to protect the client platform.

5. Security Violation

Violations of security include: sharing of user name and password pairs to provide access to an individual who has not been granted system access by a designated ROSS Accounts Manager; sharing of ROSS information or data with individuals who intend to use that data or information for purposes not within the business processes and intended use of ROSS; not following the password change procedures; and not adhering to established agency security procedures and policies. Any violation of security policies or procedures shall be promptly reported and documented to the unit security officer. Unit security officers shall report security violations to the ROSS security officer (Steve Simon 406-657-6800) or the ROSS Helpdesk (866-224-7677).

6. Service Outage Reporting

The availability of the ROSS System is a concern to all users. All users are responsible for ensuring that system outages shall be promptly reported to the ROSS Helpdesk (866-224-7677). The ROSS Helpdesk checks the availability of the ROSS application at the beginning of each business day and monitors the availability of the ROSS system at random times during the business day.

I acknowledge receipt of, understand my responsibilities, and will comply with the Rules of Behavior for the ROSS.

Signature of User

Agency

Date