

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 responsibilities of 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 users specific agency with recommendation of the ROSS Security Officer and/or USDA National Information Technology Center Security Officer (NITC). 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, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot checks to determine that an adequate level of compliance with security requirements exists. 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 ROSS's security posture.

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 (National, Regional, State, 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. Work at home

4/8/2003

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

4.2. Dial-in access.

Agency IRM Director may authorize dial-in access to ROSS from locations where network access is not available. It is understood that dial-in 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 the employee's office during network outages. If dial-in 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-in lines, and to assure that the proper level of service is provided. All dial-in calls will use username/password pairs that are managed by the National Interagency Coordination Center. If dial-in access is allowed to other applications on the system on which ROSS resides, the managers of those applications shall be notified.

4.3. Software Licenses.

All software licenses associated with the ROSS Commercial Off The Shelf (COTS) software are complied with by ROSS, as well as by contractors responsible for developing and maintaining ROSS. Personnel using ROSS are not required to physically have software licenses to use ROSS.

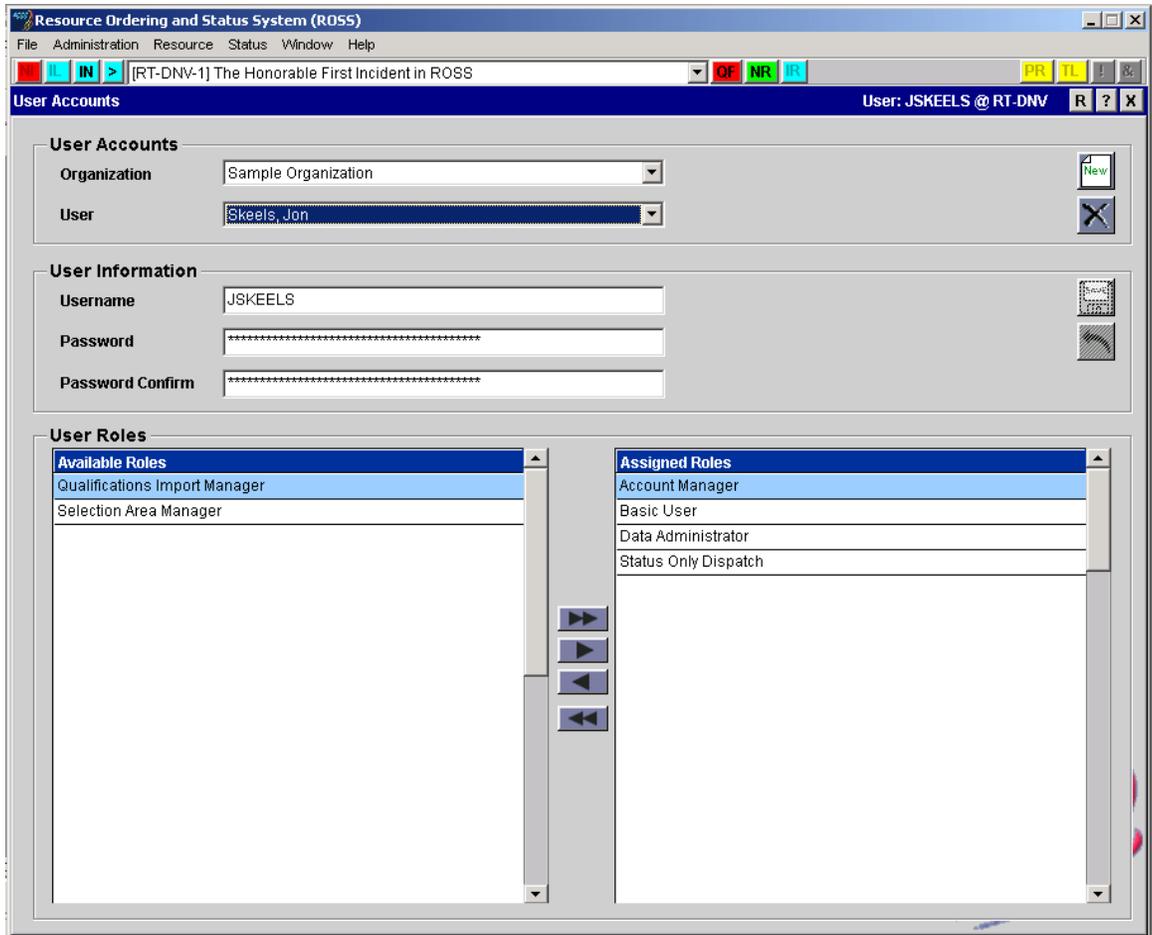
4.4. Unofficial use of government equipment.

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

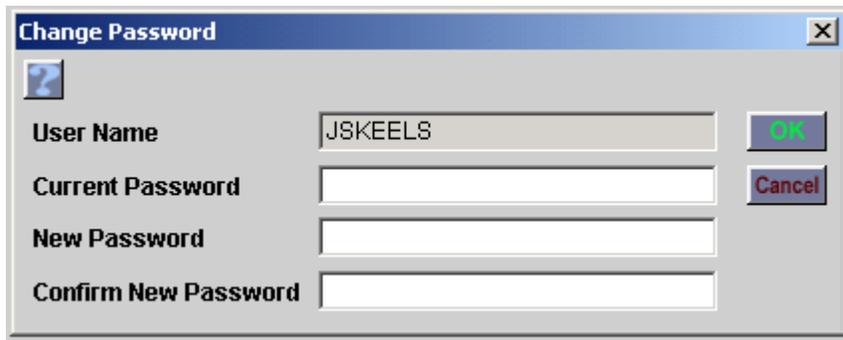
4.5. Use of passwords:

Users are to use passwords of a mix of at least six (6) alpha and numeric characters, they are to keep passwords confidential and are not to share passwords with anyone. Users shall change their passwords every 30 days.

User names and passwords are initially created/set by the ROSS Account Manager using the Account Manager Module screen depicted below. Instructions on the proper use of this screen are documented in the ROSS User Guide and Roles & Responsibilities document.



Users can change their passwords by selecting the change password function from the File drop down menu as depicted below:



4.6. System privileges

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

User accounts are can be requested through the local ROSS Account Manager.

4.7. Individual accountability

Users will be held accountable for their actions while using ROSS. This is stressed during 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 username/password pairs which to provide access to an individual who has not been granted system access by a designated ROSS Accounts Manager, sharing of ROSS information/data with individuals who intend to use ROSS data/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 Help Desk at (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 monitors the availability of the ROSS system at random times during the business day. The Helpdesk, checks the availability of the ROSS application at the beginning of each 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