

# Rules of Behavior

**Resources Information Management System (RIMS)  
NWS Data Warehouse  
Cost Management Reporting  
Cost Management Labor Survey  
Business Objects Development/Reporting Environment  
Web Intelligence Reporting Environment**

## 1. Introduction

The following rules of behavior are to be followed by all users (Government employees and contractor staff) of any of the applications that are part of the Resources Information Management System (RIMS). RIMS applications include the **RIMS Budget Formulation Model**, the **RIMS FIMA Monthly Variance Reports**, the **RIMS CAMS Monthly Variance Reports**, the **RIMS CAMS Transaction Level Reports**, the **Cost Management Reports**, the **Cost Management Labor Survey**, the **NWS Data Warehouse** including **Cost Management Data**, the **Business Objects Development and Reporting Environment**, the **Web Intelligence Reporting Environment** and the NWS table of organization application, **SPIDER**.

The rules clearly delineate responsibilities of and expectations for all individuals with access to any RIMS application. Non-compliance with these rules will be enforced through sanctions commensurate with the level of infraction. 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. Users are any individuals who access and/or utilize RIMS resources.

## 2. Responsibilities

- a. The RIMS Program Manager is responsible for ensuring an adequate level of protection is afforded to NWS Financial and Human Resource data in the RIMS production, test and development environments, through an appropriate mix of technical, administrative, and managerial controls. Users shall comply with these controls.
- b. Users of the RIMS production test and development environments are responsible for ensuring that they protect the information technology resources and assets made available to them to perform their official duties.
- c. Users who become aware of a security violation shall notify the RIMS Program Manager.
- d. Contractors supporting the NWS in any capacity who require access to RIMS data or applications are responsible for ensuring that Government information technology resources provided to them are used only in the performance of assigned tasking.
- e. Contractors acknowledge that they are granted access to licensed

software and shall honor and abide by the Government's license.

- f. Users who require access to data which includes private information about NWS employees are given this access under the condition that the data is to be used only in the performance of their duties and not for any other purpose. Further, users shall comply with the Privacy Act and safeguard any data provided to them. Disclosure of confidential data, employee information, or bureau specific data is forbidden.
- g. Users shall only access, or attempt to access systems/servers they have been explicitly authorized to access.
- h. The RIMS Program Manager will grant a default password to users at the time a new user account is created. Users must change the default password to a password which conforms to DOC, NOAA and NWS password policies the first time they logon. Passwords will expire and users must create new ones to replace them every 90 days. Users shall safeguard their passwords and not share them with any other person or organization.
- i. Access to RIMS resources shall be restricted to official business only. This access shall not be delegated, shared, or provided to any other user without authorization from the RIMS Program Manager.

3. Other Policies and Procedures

These rules are not to be used in place of existing NWS or NOAA policy, rather they are intended to explicitly define the rules each user must follow while accessing NWS or NOAA Financial and Human Resource data. The rules are consistent with the policy and procedures described in the NOAA Computer Security Handbook. The Handbook contains computer security guidance on a wide range of topics (i.e., personnel security, incident handling, and access control mechanisms). This document contains responsibilities for the RIMS Program Management, RIMS Development and Operations staff and RIMS users.

4. Unofficial Use of Government Equipment

Users should be aware that personal use of government-owned information resources, including hardware, software and data, is not authorized.

5. Acceptance of Rules of Behavior

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

\_\_\_\_\_  
Signature of User

\_\_\_\_\_  
Date