SUNY RF
The Research Foundation for
The State University of New York

# The Research Foundation for The State University of New York Campus Security Administrator Handbook

## Table of Contents

## Introduction

The campus security administrator ensures that users have the appropriate access to the Research Foundation for SUNY's (RF) business applications. This document describes the campus security administrator role and includes the processes that should be followed in this role.

## Campus Security Administrator

### Responsibilities

The campus security administrator is responsible for the following:

- Ensuring users have the appropriate access to the RF systems:
  - Access necessary to perform their jobs
  - Access that does not cause segregation of duty issues
- Ensuring access is terminated on a timely basis
- Monitoring access

The campus security administrator must follow the policies and procedures as outlined in this manual.

### How to Appoint

Campus management designates a campus security administrator through the annual signature delegation process as outlined in the Signature Delegation Procedure. If changes occur during the year, the Operations Manager (OM) or delegate must update the form and send it to the RF's Office of Compliance Services.

Campuses should also determine if they would like to enter the information in the business applications security module or have Customer Services do it. The campus security administrators should log a help desk ticket with Customer Services if he or she does not have the Oracle responsibilities and training needed to enter information in the security module.

### Oracle Business System Access for Security Administrators

The campus security administrator will need one of the following Oracle responsibilities to perform the requirements listed in this manual:

- ORG Campus Security – this is for campus security administrators who enter information in the security module.
- ORG Campus Security Inquiry – this is for campus security administrators who do not enter information in the security module and for those who are responsible for monitoring campus security administrator activity.

## New Access

A new RF employee, principal investigator (PI), project support staff, or SUNY/RF administrative staff responsible for RF business at the campus will need access to the RF's business applications when they start their job. HR staff must enter the user into the Oracle HR module before the campus security administrator can give the user access.

Campus security administrators should work with campus RF HR staff to ensure there is agreement on the process and timing of adding someone to the Oracle HR module. Once HR enters the person's name, social security number and campus location into Oracle a process runs every 15 minutes to create a RF user ID for the person.

### Using Campus-Assigned User IDs

Certain campuses allow PIs, project staff and administrators to use their campus user ID and password to access to the RF Report Center and Effort Certification and Reporting Technology (ECRT, see page 7). This is done via the single sign-on InCommon solution. For these campuses, the individual's LDAP ID must be added to the individual's person record for this authentication to work.

An LDAP ID is the equivalent of a user's campus Net ID plus @campusname.edu, e.g., johnsmith@albany.edu. Anyone with an HR responsibility or with the XXX Sign-on and SUNY Job Information responsibility can add this information.

### Informing Users of their RF User ID

- RF Employees: If an e-mail address is entered in the HR module, they will receive a welcome e-mail with their user ID and directing them to finish the authentication process and set a password.
- SUNY Employees using Campus User ID and Password: If your campus uses the InCommon single sign-on solution to access ECRT and the RF Report Center you do not need to inform the individual of their RF user ID. **Note**: If the individual needs to access other applications, e.g. Oracle, you will need to inform them of their RF user ID as per the below bullet.
- SUNY Employees using RF User ID: For all other campuses or for those that need access to applications other than ECRT or the RF Report Center, campus security administrators should inform users of their RF user ID and provide them instructions to finish the authentication process and set a password.

### Completing Authentication and Setting a Password

Users will need to complete an online form to complete authentication and to set their password for their RF user ID. Campus security administrators should share the steps listed in Appendix A, "Self Registration," to help users complete this process.

### Granting Access to Applications

Once a user ID is created, the campus security administrator can assign access to the RF's business applications (see below). Users will need a completed Project Staff User Access Form or Administrator User Access Form before campus security administrators can assign them access.

- Oracle Business System – the application allows access to RF grants, financial, HR and payroll transactions and data
- RF Report Center – allows access to the RF's reporting application. Data from the Oracle Business System is retrievable in this module.
- Web Financial Reports

- Payroll Reports – this application gives access to specific payroll reports that are run immediately after payroll for reconciliation and reviewing purposes.
- ECRT – the online tool the RF uses to certify and monitor certification of effort statements.
- E-mail groups – the RF offers several groups by role (e.g., Accounts Payable, Sponsored Programs).

### Automatic Access

RF employees and supervisors of RF employees are automatically assigned self-service (i.e. Employee Self Service, Supervisor Self Service) responsibilities. The campus security administrator does not need to take further action if the employee or supervisor does not need access to other RF business applications. These responsibilities do not need to be included in monitoring reviews.

PIs may have access to the PI Dashboard for those projects/awards for which they are identified as a PI. Refer to the "Understanding RUSAM" section below for information on how to set this up. This access is not automatic but no approval or documentation is needed to give this access. Campuses should establish a process they are comfortable with to give PIs this access.

All other access should be granted only after completion of the User Access Form.

### User Access Form for all Other Access Requests

Users will need a completed Project Staff User Access Form or Administrator User Access Form to get access to the RF's business applications. The appropriate form is required for all users except those listed in the Automatic Access section above. Campus security administrators are responsible for:

- Reviewing the form.
- Ensuring all campus approvals are documented.
- Determining that the access requested is appropriate for the job and that there are no segregation of duty issues.

Campus security administrators that enter information for their campus can then follow the steps in Appendix B, "Oracle Input and Running Reports Steps," to set up the access. Otherwise, campus security administrators should forward the form to Customer Services for input. In either case, the form must be kept for the length of the user's access plus 1 year. Documentation may be subject to audit.

### Understanding RUSAM Functionality

The RF uses a custom solution, called RUSAM, to ensure project and administrative staff have access to only the data for which they are responsible. RUSAM does not restrict the data for HR responsibilities; it will only govern the data seen for those with Oracle responsibilities that start with "ORG" or "KEY", or RF Report Center responsibilities. A users security settings are established in the RUSAM form by using three components:

- User Location
- Access to Labor Costing on Grants Module
- Award Information Interface

User Location: The value entered in this field will apply to the Oracle applications for responsibilities that start with ORG.

Access Labor Costing on Grants Module*:* These check boxes work in conjunction with the security assigned in the "User Location" and "Award Information Interface" sections by further restricting access to salary detail on RF Funded or Corporate Funded awards. By leaving these boxes unchecked, the user will not be able to see salary detail in the RF Report Center for RF Funded or Corporate Funded awards even if they have access to these awards. They will be able to see salary detail for all other awards, summary salary data for these types of awards, and salary detail in the Oracle applications. If the user needs access to salary detail on either one of these awards, check the box. See Security Terminology below for more information on Labor Costing.

Award Information Interface

*Security Type*

- **Award** - Access to award level data and all associated projects and tasks on the award.
- **Project** - Access to project level data and all associated tasks on the project.
- **Task** - Access to task level data and all associated sub-tasks.
- **Organization** - Access to all data pertaining to the user's assigned organization level as defined in the HR hierarchy of subordinate organizations. A user could have access to all awards, projects and tasks at the campus or the departmental level. This is the highest level of access.
- **Key Member** - Access to awards and/or projects and tasks for the person listed as the Key Member on a project, Task Manager or Personnel on the award.

*Security Value*
This is the value of the above chosen security type. (e.g., Award = 12345, ORG = 010 University Center at Albany, Key Member = Doe, John Dr.).

*Task Project Value*
This value is used when the security type Task is chosen to identify what project the task value is associated with (e.g., TASK PROJECT VALUE = the project and SECURITY VALUE = Task).

### Oracle Business System, Report Center and Web Financial Reports

Access to the Oracle Business System, RF Report Center and Web Financial Report applications is controlled through assignment of responsibilities that are added to users' records in the Oracle Business System.

Although campuses can enter many responsibilities, some require additional approval.

Campus Security Administrators must send in a separate request for Customer Services to add the user to the buyer file if the user has any of the following responsibilities:

- ORG Purchasing Specialist
- ORG Purchasing Administrator
- ORG Purchasing Buyer

In addition, if they have these responsibilities they may also need an electronic signature added to the system to electronically approve purchase orders. The purchasing supervisor must approve electronic signature requests.

RF Report Center and Web Reports responsibilities assigned to users will not be available until the next business day because the information in these applications requires a nightly replication before they are updated.

### Payroll Reports

Payroll reports are available through special access to the RF Web site so that campuses can review payroll input and errors for their location on a bi-weekly basis. Only users with a business need to know should be granted this access. Approvals must be obtained from the Campus Payroll Officer and the Central Office Payroll Manager before access is granted.

The Campus Security Administrator must submit a request to Customer Services via e-mail. The request can also come from the HR/payroll office; however, the campus security administrator should be copied. Customer Services will forward the request to the Central Office Payroll Manager to obtain approval from the Campus Payroll Officer as it is strongly recommended that the campus human resources office approve this type of access.

After all approvals are granted, Customer Services will grant access to the user, this cannot be done at the campus level. Approval documentation does not need to be forwarded to Customer Services.

### Effort Certification and Reporting Technology (ECRT)

ECRT is used to certify effort statements for those who have effort on sponsored programs. Individuals who will certify effort or others who perform effort-reporting administration will need a role in ECRT. Campuses should send an e-mail to effort@rfsuny.org to request that a role be assigned to an individual.

## Modifying or Terminating User Access

It may become necessary to modify or terminate access to the RF business applications if a user leaves employment or has a change in position.

Campus security administrators are required to remove or send a request to remove all responsibilities except Employee Self Service to RF business application access for users who no longer require access due to job change, leave of absence or separation from employment. Campus security administrators must establish a process to remove such responsibilities.

They should also notify Customer Services so that Customer Services can perform the following:

- Remove users from e-mail groups or listservs
- Remove users from the buyer file if they have purchasing responsibilities (see list on page 8)

The same steps should be followed if the user changes jobs, except the responsibilities should be adjusted if they still need some form of access to perform their new job responsibilities.

### Password Violations

A user account is "locked out" of the RF Web site after five unsuccessful login attempts. A user who is locked out should use the "Forgot Password" feature. The user will be sent an e-mail with a temporary password that the user should use to login and immediately change using the "Change Password" feature.

The user should contact Customer Services if this does not work.

## Monitoring

### Monitoring Campus Security Administrator Activity

Campuses must run the "RF Campus Security Audit Report" on a periodic basis, no less than monthly, to monitor security administrator activity in the Oracle applications. This report documents security changes made in the Oracle applications and should be reviewed to ensure the activity is appropriate. Campuses should evaluate the frequency the review is performed based on other campus controls, meaning if each business function is monitored for irregular transactions, this report could be run less frequently. Generally, someone without the ability to enter changes should perform this monitoring activity. The responsibility "ORG Campus Security Reporting" can be used for this purpose.

If an unauthorized or inappropriate change was made, campus management should be informed immediately and should refer the matter according to the Fraud and Whistleblower Policy.

### Annual Campus Review of User Access to the RF Business Applications

Campuses must run the "RF User Report" annually to monitor users registered in the application security system to verify correct access. This ensures that the RF's internal control environment is appropriate and effective. In addition, if a campus has local systems that stores RF information annual reviews of access to these systems should also be performed and documented.

Campus security administrators must provide written confirmation of the review to the RF's Central Office Information Security contact each year. Central Office will start the annual review process by sending an e-mail to campus security administrators with the deadline for the review. Documentation of review may be subject to audit.

The following areas must be evaluated as part of the annual review:

1. There is an ongoing need for a user's access to RF data (e.g., active user account, current employment).

2. User must have appropriate data access for his or her job role(s), including inquiry access versus update access.
3. Segregation of duties is appropriate for the user's access.
4. Access to human resources data is restricted to only those personnel for whom it is essential in relation to their job duties.

### Other Optional Monitoring

The RF provides security reports to ensure access is controlled, accurate and to help avoid misuse. The campus security administrator is responsible for monitoring access to the RF business applications for users at their location to protect RF systems and data.

- RF User Report: As stated above, this report should be run annually at a minimum. However, this report can be used more frequently to monitor access, particularly for those with access that allows them to make changes in Oracle. The report is in Excel and can be sorted and manipulated to meet the monitoring needs for your campus.
- RF Responsibilities Report: This report should be used to view users who are assigned a specific responsibility.
- RF Stale Login Report: This report can be run to determine if users of the Oracle Business Applications have not a particular number of days.

### Documenting and Retaining All Security Monitoring Reports

The RF provides the "RF Business Applications" and "Web Site Security" reports to ensure access is controlled, accurate and to help avoid misuse.

Campuses should retain reviewed reports for audit purposes for three months. Campus management can determine that three months is unnecessary but the minimum length of time cannot be less than one month. Documentation of review may be subject to audit.

## Contact Information

### Where to Go for Help

If you have questions, you can seek guidance from Customer Services.

## Security Terminology

**RUSAM Location Code:** The unique campus identifier (three digit code) limits a user's ability to view and/or change data to a specific location. RUSAM location codes do not apply to Human Resource responsibilities (see responsibility definition below).

**Person Record in HR:** Users must be defined in the People table in the Human Resources (HR) module in order to allow access to all the data and forms within Oracle and the RF Report Center.

**Labor Cost:** Allows or restricts labor expenditure details for RF Funded or Corporate Funded award types, for use *with a grants responsibility* only. Funded security access allows a user access to individual salary and wage information on an award. For salary detail security restriction, awards are segregated by purpose code. The purpose codes determine whether salary and wage information is restricted on a type of award. There are many purpose codes, but only the following three are restricted and require RF and or Corporate Funded access:

| Check box | Award Purpose Code |
|---|---|
| Corporate Funded | Corporate GL Holding<br>Central Office Administration |
| RF Funded | RF Funded Revenue |

A campus **CAN** have Corporate Funded access in order to view their Corporate GL Holding (purpose code) vacation accounts. This access applies only to those corporate funded accounts with an ORG code of the specific campus location. In other words, a specific campus user is only going to be able to view salary and wage information on his or her campus accounts. The security logic of an ORG or KEY responsibility still applies—if a user has a KEY responsibility and is not listed on the vacation award in a grants "Role" that user will not see the award.

**A to B Renewal:** A to B is a grants process to transfer labor schedules from one award/project/task to another award/project/task when certain criteria are met to run this process for payroll purposes.

## Appendix A – Self Registration

Go To www.rfsuny.org.

1. In the upper left hand area of the homepage, access the Login button.
2. Click the "Request Access to the RF Web site."
3. Complete the online **registration** form, entering the following information (required information noted by an asterisk):
    - Title
    - First name*
    - Middle name
    - Last name*
    - Phone number*
    - Last 4 digits of Social Security Number* (For RF employees this will speed automatic approval)
    - Campus name*
    - E-mail address* (this will be used for communications regarding your user id – will not be used for any other purpose)
    - Desired password
4. Click the **Submit** button at the bottom of the form.

## Appendix B – Oracle Input and Running Reports Steps

### Assign access

1. Open the User form (Oracle Security>User>Define)
2. Query the user: View>Query>Enter or F11
3. Enter the user ID in the User Name field
4. View>Query>Run or Ctrl+F11
5. In the bottom of the "Direct Responsibilities" form add the appropriate responsibility from the list
6. Save

### Terminate access

Follow steps above until step 4

1. In the bottom of the "Direct Responsibilities" form, enter an end date in the "Effective Date To" column.
2. Repeat for all active responsibilities except "Employee Self Service" if the person is no longer part of the RF or SUNY
3. Save

### RUSAM Entry

1. Open the RUSAM form (RUSAM Security Maintenance)
2. Query the user View>Query>Enter or F11
3. Enter the user id in the User ID field
4. View>Query>Run or Ctrl+F11
5. Enter the User Location, Access Labor Costing on Grants Module, Award Information Interface according to the information on the User Security Form
6. Save

### Instructions for Running Security Monitoring Reports

1. Log in to the RF's Oracle business application and choose the responsibility ORG Campus Security Reporting > Security Notifications > Notifications
2. Select the request type **Single Request** and click **OK**.
3. Enter the report name you wish to run from the list of values in the **Submit Request** form.

a. **Copy Button Feature:** To re-run a previous report request, select a request from the list click on the Copy button. The **Copy** button will display a list of previous requests submitted from this responsibility. You may also make a change to the parameters of a previous request by clicking in the Parameters field on the Run Request form.

4. If a report requires parameter values, the **Parameters** window opens so that you can define parameters. Parameters are different for each report. *Note: for the RF User Security Report, leave the last log in to and from dates blank to ensure you get all users. These dates only work for Oracle access; they are not relevant for Report Center access.

5. Enter the values in the required parameter fields and click **OK.**
6. Click on the **Submit** button.
7. **Schedule Feature**: If you wish to define a report schedule, use this button to establish a specific time or repeatedly run the report at specific intervals. Click on the **Schedule** button to open the **Schedule** window and enter a run schedule.
8. Once a report request is submitted, you will need to click the **Refresh Data** button to view the status of the report request. Once the request is completed in the Phase column, you may click the **View Output** button to open the report.

## Appendix C – Responsibility Listings and Segregation of Duties Reference

Accounts Payment Responsibilities
Accounts Receivable Responsibilities
Grants Management Responsibilities
HR Responsibilities
LD Responsibilities
Payroll Responsibilities
Property Management Responsibilities
Purchasing Responsibilities
SUNY Payroll Responsibilities
Finance Duty Segregation Guidelines
Grants Management (OGM) Billing Duty Segregation Guidelines
Human Resources/Payroll/Labor Distribution Duty Segregation