The HRMS and FIS User Security Certification process is located within the HRMS system. To begin the certification process, logon on to the HRMS system and select the following: **Main Menu > Manager Self Service > Annual Certifications > Certify User Security.** The menu path is located within the grey menu on the top of the page. Once selected follow the steps listed below. 

If you have any questions, please contact the FIS Help Desk at 935-5707.

**PURPOSE**

Per the Guide of Internal Controls, HRMS/FIS User Security Certification was initiated to address the need to document annual reviews of HRMS and FIS user security by appropriate level of management.

**INDEX**

Steps for the Security Certification Process....................... Page 2
Queries “How to Run”.................................................. Page 5
Printing User Security Profiles....................................... Page 6
Explanation of User Security Certification Tabs.............. Page 10
STEPS

1. At the Security Profiles page, leave the search criteria fields' blank and click on search. This will result in a list of all HRMS and/or FIS users that fall within your security certification rights. You may narrow the list by using any of the search criteria fields; however, all users will need to be certified annually. Note: Certification responsibility rights are based on HRMS payroll prime and secondary job departments.

   Search Criteria:

   **User ID** = Search by User ID #
   **Name** = Search User Name, by Full Name or Last Name
   **Last Name** = Search by User Last Name
   **Department** = Search by Users within a Department
   **Reporting Level** = Search by Users within a Reporting Level
   **Job Indicator** = Search by Primary or Secondary Job
   **Show Only Certification Reqd** = Check box to search for Users who have yet to be certificated within HRMS, FIS or both, indicated by a Y in the Show Only Certification Reqd column on the search return.

Search Tip: Use % as a wildcard search character.

Search Tip: How do I know which employees need to be certified?

   **Step 1.** From the ‘User Security Profile’ page select the ‘Department Number’ or ‘Reporting Level’ or other search values.
   **Step 2.** Check the ‘Show Only Certification Reqd’ box (check is automatically defaulted). (See example below)

   ![HRMS Security Profiles](image)

   ![Search Criteria](image)

   **Show only Certification Reqd.?**

   **Step 3.** Return results are indicated by ‘Y’ in the ‘Show Only Certification Reqd’ column. All search results returned with a ‘Show Only Certification Reqd’ = ‘Y’ requires certification either in HRMS, FIS or Both.
If you uncheck ‘Show Only Certification Req’ box, then your search results will be indicated by an ‘N’ in the ‘Show Only Certification Req’ column. No further action is required on your part, these individuals have already been certified or no certification is required (employee has HRMS EE Self Help and either no FIS access or both).

2. From the search results, select a user. This will return you to the User Security Profile composed of two tabs: HRMS Profile and FIS Security. The individual tabs are described in detail on page 10. For information explaining each function available for HRMS and FIS, please click on the HRMS Roles Tab, located on the right or FIS Function Descriptions link located in the upper right hand corner on the FIS Tab.

3. Review security rights assigned to the user for appropriateness, based on assigned duties and responsibilities. Please note: if an employee has only HRMS self-service (WP EE Self Help) and HRMS employee time and labor self-time (WP T&L Employee) or no FIS access, certification is not required and will be auto certificated “HRMS or FIS Certification Not Required.”

   See Printing User Security Profiles (Pages 6-9) for printing instructions and options.

4. To remove inappropriate security access follow these steps:

   Step 1. Print a copy of the report by selecting the “Printer” icon from the security profile page. Or, see Printing User Security Profiles (Pages 6-9) for printing instructions and options.

   Step 2. Draw a single line through each security function line to be removed and indicate “Delete.”

   Step 3. Sign the user’s security profile page. Please note the form must be must be signed by an authorized manager.

   Step 4. Fax the user’s security profile page to the FIS Help Desk at 935-8619.

   Step 5. Once the changes have been completed by the Help Desk, review the changes and certify the user in HRMS.

   Please note: Changes other than deletions must be submitted on the appropriate HRMS or FIS Security Authorization form. A link to the appropriate form is provided in the upper right hand corner of each tab (HRMS or FIS Security Form).

5. Once you are comfortable that the user’s security is appropriate, based on assigned duties and responsibilities, click on the yellow certification statement, located at the bottom of the page. After you click the certification statement, your name, date and time will be displayed in the certification fields. **The certification must be completed on both the HRMS and the FIS tabs.** When you are finished, you may click on “Next in List” or “Return to Search” depending upon your original search criteria (located at the lower left hand corner).

For employees with Primary and Secondary Job Indicators, it is the responsibility of the employee’s Primary Department to complete the Security Certification.
**Important Note:**

For internal control purposes, the system prevents users from certifying their own security. As a certifier, you should review your own User Security Profile and make corrections, if applicable. After your profile has been updated, you should print and sign the profile, “certifying” that the access you have is reasonable and necessary.

- Users from the Medical School, who are restricted from certifying their security, should fax their signed profiles to Mary Corcoran at 367-6666 or send by email to marycorcoran@wustl.edu.

- Users from the Danforth Schools and the CFU, who are restricted from certifying their security, should fax their signed profiles to Kristen Singer at 935-4811 or send by e-mail to kristen.singer@wustl.edu.
How To Run Queries

A query has been designed to assist you with the Security Certification process (located within “Security Cert” folder).

To run the query, click on “Queries” (located in the gray menu box on the top of the page), then click on “Query Manager”. Using the “Search by: Query Name Begins with Option”, type in either the full or partial name of one of the query listed below that you wish to run and click ”Search” (you can also leave the field blank for a list of all available queries). Locate the specific query you want to run and click on the “Run to HTML” or “Run to Excel” link.

1. **WP_DP_SECURITY_CERTIF**  This query displays a list of all users, within your area of responsibility, that have security access to HRMS and/or FIS. In addition, it displays the most recent certification date, if applicable.

   **Note: Users who only have security access to HRMS Self Service are excluded from this report.**

   The query can be run for a single department, a range of departments or by reporting level. To run the query for a single department or a range of departments, you must fill in the “from” and “thru” fields on the query selection page.
**Printing User Security Profiles**

**“Printer Friendly Version”**

A printer friendly version of one user security profile may be printed. Click on the “Printer” icon button located in the upper right corner of the User Security Profile Page. Clicking on the “Printer” icon button will open a new window. The new window is a .pdf printable version of the currently open User Security Profile Pages. The file then can be either (1) printed or (2) “Saved As” and emailed.

**“User Security Profile Report”**

A second report option allows you to schedule one or more security profiles reports that may be printed. To access this option to print multiple User Security Profiles, select Main Menu>Reports>User Security Profile Reports.

To schedule a report job, follow the steps listed below:

1. Select “Add a New Value” located at the bottom right of the page.

2. At the “Run Control ID” prompt, enter a unique identity, such as your initials, and click on the Add button. If you already have a Run Control ID, click on the Search link and select it.
3. At the drop down box, next to the BY prompt, select Department ID (to print all profiles for a specific department number), User (to print a profile for a specific empl ID –search either by empl ID or name (first and last)) or Reporting Level.

4. Click on the “Run” button located at the top right of the page. This will take you to the Process Scheduler Request page. Click on the “OK” button located at the bottom left of the page.
5. Click on the “Process Monitor” link at the top right of the page.

6. Under the process list, look at the report status for the process name “WPUSRSP”. The report request will have an initial Run Status of “Queued.” Periodically (after a minute or so), click the “Refresh” button at the top right of the page to update the Run Status field. Once the run status displayed reads “Success”, and the Distribution Status is “Posted” click on the “Details” link. This will then display the Process Detail page.
7. On the Process Detail page, click on the “View Log/Trace” link at the bottom right of the page.

8. On the View Log/Trace page, click on file link ending in “.PDF” under the “File List Name” section of the page. A new window will open with the printer friendly PDF file, print the report.
Explanation of the User Security Profile Tabs

There are two tabs on each user security profile. The HRMS Profile and FIS Security, contain detailed information about specific security rights the user has. The following explains each section under the HRMS Profile and FIS Security tabs:

- **HRMS Profile**
  - **Basic Information** ➔ Contains basic information recorded in HRMS, as well as the last date/time signed on to HRMS and the last date/time the user’s HRMS password was changed.
  - **Security Roles** ➔ Roles determine the functionality for each user and contain the “logical” grouping of pages (functionally). All Roles begin with ‘WF’ (Workflow) or ‘WP’ (Non-Workflow).
  - **Job Department Access** ➔ List of departments for which the user can access employee data. Users have access to all departments shown unless the Access column reads “No Access”. Rollup Departments are used when the user has access to all departments within a higher level --- such as Surgery or Internal Medicine or School of Business.
  - **Source Department Access** ➔ List of departments for which the user is authorized to assign sources. This does not mean they can view all distributions to those sources. Users have access to all departments shown unless the “Access” column says “No Access”.
  - **Restricted Funds Access** ➔ If funds are listed, the user can source to only accounts that contain the fund number listed. This does not mean they can view all distributions to those funds. Users have access to all funds shown unless the “Access” column says “No Access”.
  - **Workflow Roles and Routing Depts** ➔ This section displays each of the Workflow Roles for the user, if any. The “Route Control” column shows the departments applicable to each Workflow Role.

- **FIS Security**
  - **Document Access** ➔ This section displays the documents/functions and the corresponding department the user may access.
  - **Inquiry and Other Access** ➔ This section displays the department numbers included in the document access function.
  - **Account Inquiry** ➔ The account inquiry section lists the ledger classes accessible in the Account Inquiry view.
  - **Accounts Payable Access** ➔ This section lists rights within the accounts payable function by document/function and department.
  - **Approval Authority** ➔ This section displays document approval levels by document/function, ledger and class, department, fund, budget/object code, and by dollar limits. “X” represents a wildcard for all.
  - **CFU Functions** ➔ This section displays administrative functions generally limited to CFU departments such as Accounts Payable.
  - **Miscellaneous Access** ➔ This section displays general rights such as the Department Lookup or User Options Menu.