Business Officer User Manual – Security Administration

Financial Systems Tools (FST) Addendum

The University of Iowa

Accounting and Financial Reporting (AFR) impacted applications

Table of Contents

Section 1: FST User Guide

Purpose of this User Guide

This addendum identifies the additional security administration functionality available to Business Officers and their Administrative Delegates in Financial Systems Tools (FST). Various reporting and transactional applications supported by the Finance and Business Information Services (FBIS) development team and specific Accounting and Financial Reporting (AFR) owned reporting and transactional applications are included. Please note that the term "Business Officers" in the context of this user guide, includes their Administrative Delegates as having the same functionality available to them.

For basic FST functionality please refer to the campus FST User Guide.

Section 2: Security Model Introduction

Access Groups

An Access Group is reserved for granting access and/or eligibility to specified types of applications based on the Access Group you are granted.

EFR (Electronic Financial Reports) Access Group & Financial Reporting (AFR) application

The EFR Access Group in conjunction with the Financial Reporting (AFR) application is a base level role whose main purpose is to grant access to the EFR Portal and other reporting-based applications, along with granting eligibility to other subsidiary reporting and transactional applications that are further restricted and require separate access request forms.

The elements of the FSM are described below. A diagram is also provided further below.

Security to this group grants the user access to the following applications in Employee Self Service:

- ✓ Electronic Financial Reports (EFR) Portal (Transaction Detail Reports (TDR), Summary Reports, Dashboards, General Ledger (GL) Reports & Grant Reports)
- ✓ Financial Systems Tools (FST)
- ✓ Request for GL Chartfields & WhoKeys
- ✓ WhoKey Administration

Security for this group grants a person **eligibility** to the following applications in Employee Self Service; however, security for each application must be granted separately through the security mechanism used for that application:

- ✓ Cumulative Compensation (CumComp)
- ✓ Grant DSS (supported by the Grant Accounting Office)

Access grants a person **eligibility** to the EFTx Access Group.

Access is automatically granted to users with the following roles:

- ✓ WhoKey Administration Roles (Owner/PI, Reviewer, Secondary Reviewers & Research Administrators)
- ✓ Institutional Roles (Business Officers, Departmental Executive Officers & Research Administrators categories)
- ✓ Transactional applications including PayCV, WebCV and GL Journal Entry (GLJE)

If a user does not have one of the above roles and needs access to the EFR Access Group, then the *Financial Reporting (AFR) application Request Form* found in FST can be completed to request access for that individual. This form is only visible to Business Officers to prevent unnecessary requests by campus users that don't have the full understanding of the security model. **Please remember it should be rare to request this group alone.**

If you have questions please contact AFR-ElecFinTrans@uiowa.edu.

EFTx (Electronic Financial Transactional Applications) Access Group

The EFTx Access Group is another base level role whose main purpose is to grant eligibility to transactional applications that are further restricted and require separate access request forms.

Access automatically grants a person the EFR Access Group.

Security for this group grants a person **eligibility** to the following applications in Employee Self Service; however, security for each application must be granted separately through the security mechanism used for that application:

- ✓ PayCV
- ✓ WebCV
- ✓ GL Journal Entry (GLJE)

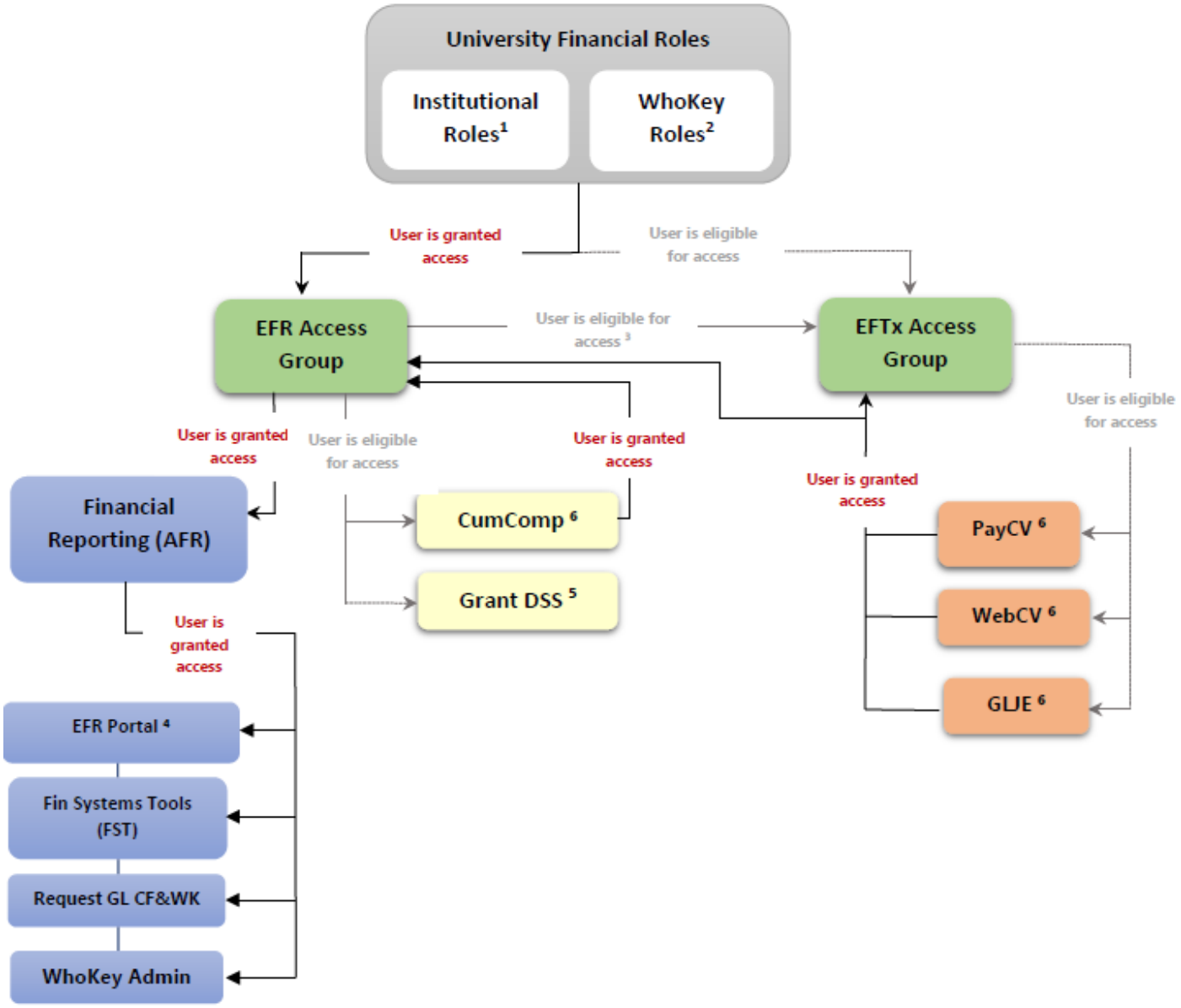
Access is automatically granted to users with roles to the following transactional applications:

- ✓ PayCV
- ✓ WebCV
- ✓ GL Journal Entry (GLJE)

NOTE: EFTx Access Group cannot be granted to a person through any access request form. It is not necessary to grant separate access to this group because it is a secondary high-level role that by itself does not gain the person access to any specific application.

Financial Security Model (FSM) Diagram

Accounting and Financial Reporting (AFR) impacted applications supported by FBIS



[1] Business Officers, Departmental Executive Officers & Research Administrators categories
[2] Owner/PI, Reviewer, Secondary Reviewers & Research Administrators
[3] EFR Access Group grants eligibility to EFTx Access Group; EFTx Access Group grants access to EFR Access Group (example: user has no prior access and is granted PayCV application access, the user will be granted EFTx & EFR Access Groups).
[4] Includes TDR, Summary Reports, Dashboard, GL Reports & Grant Reports.
[5] Grant DSS is supported by the Grant Accounting Office.
[6] Required Workflow based access request forms available in FST.

Section 3: Additional Menu Options

As a Business Officer or Administrative Delegate you will have access to additional functionality in FST that will allow you to manage security for your staff.

Home Page Sub Menu Options

Security

Request Application Access:

- ✓ ***Financial Reporting (AFR):*** Request form will only be available to Business Officers and Administrative Delegates. It is **rare** that anyone needs granted the base level Financial Reporting (AFR) application (includes EFR Portal, FST, Request for GL Chartfields & WhoKeys and WhoKey Admin) access by itself due to the user having been granted access to it through one of the following roles/applications:
  - WhoKey Administration Roles (Owner/PI, Reviewer, Secondary Reviewers & Research Administrators)
  - Institutional Roles (Business Officers, Departmental Executive Officers & Research Administrators categories)
  - Transactional applications including PayCV, WebCV & GL Journal Entry (GLJE)

  It is recommended to review the person's access first to see if they already have access. If you are still not certain what to do, please contact AFR-ElecFinTrans@uiowa.edu.

User Lookup: Allows you to search for your employees in order to view their security page.

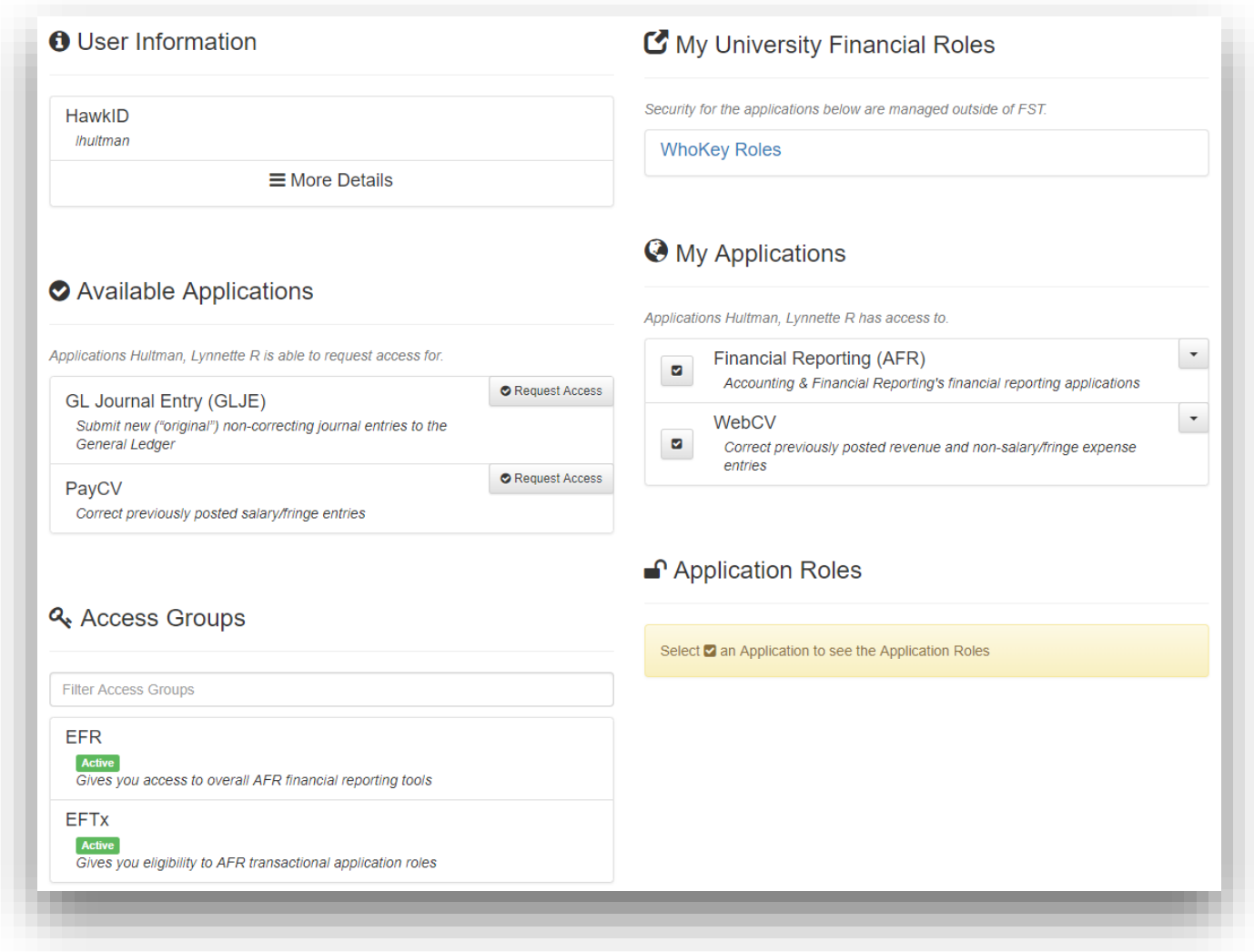
Reports: Various security reports based on the individual's primary HR Org-Dept.

- ✓ ***Access Group User List:*** List of users who currently have access to Access Groups EFR and/or EFTx.
- ✓ ***Application User List:*** List of users who currently have access to PayCV, WebCV, GLJE and/or CumComp applications.
- ✓ ***Transactional Application User List and Year-End Privilege Information:*** List of users who currently have access to PayCV, WebCV and GLJE applications and if they have Period 14 permission for the application.

NOTE: With the ability to pull security reports on demand, AFR will no longer send the annual security review or Year-End Privilege emails. Business Officers will be responsible for completing this review.

Section 4: My Security Page

You will access this page by either selecting the "My Security" option in the Main Menu or when you complete the "User Lookup" in the Sub Menu Options (homepage).



Search: To the left of the user's name at the top of the page there is a button with two arrows that cross. Select this to search for another individual's security page.

User Information: Section may be expanded to show more details that help identify the person you are reviewing. Details include HawkID, University ID, Employee ID, Org-Dept, Position Number and Company.

Available Applications: Provides the list of applications the person is eligible for but does not have access to now. A "Request Access" link appears to request access to that specific application. This section will only appear if there are applications the person does not have access to.

Access Groups: Provides the list of Access Groups that the individual has access to and provides the status

the person has for those roles.

- ✓ ***Active:*** User currently has the Access Group.
- ✓ ***Suspended:*** Due to a transfer where the individual's Position number changed, the user's access will be put into a 7-day suspension. This will prevent the user from accessing any applications while allowing the Business Officer/and their Administrative Delegates or the Department Admins/and their Delegates the chance to review and determine if the person's access should be reinstated. If not reinstated within the 7-day suspension, then the person's access will be revoked.
    - ***Down arrow button (right of Access Group name):*** If access needs reinstated, select the down arrow to the right of the Access Group and select "Grant". Per business rules, if the person has both EFR and EFTx Access Groups, if you reinstate EFTx first, EFR will automatically be reinstated. If you reinstate EFR first, then you will have to manually reinstate EFTx. Please note when you grant the Access Group(s) back, the associated applications will also be granted back.
- ✓ ***Revoked.*** Due to a 7-day suspension expiring, a transfer where the individual's Org and Position number changed, or a termination, a person's access will be revoked to all Application and Access Groups.

My Applications: Provides the list of applications that the individual has access to. There may be two sections, one section will list the applications that are currently handled through the new Security Model. The second section will list the applications that are not currently handled through the new Security Model but will be soon.

- ✓ ***Checkmark button (left of application name):*** Selecting this option will then display the Application Roles section below My Applications and will list the roles the individual has access to for the selected application.
    - ***Add Roles:*** For GLJE, PayCV and WebCV applications you will have the ability assign the Period 14 application role. If the user does not have the role and you select the "+" button to the right of the "Application Roles" title you will have the option to add the role, completed by selecting the role in the "Existing Application Roles" column and selecting "Add". If no roles are available for you to manage, then you will receive a message stating this.
    - ***Remove Roles:*** For GLJE, PayCV and WebCV applications you will have the ability to remove the Period 14 application role. If the user has the role listed in their "Application Roles" section you will see a red "x" option, upon selecting and confirming will remove the role.
- ✓ ***Down arrow button (right of application name):*** You will have two options:
    - ***Request Application Roles:*** Shortcut to the application's access request form. Your name will be defaulted to the form but can be updated to another individual that you may be requesting access for. This can also be used to request for additional roles, such as Period 14 access that the person you are reviewing doesn't yet have access to.
    - ***Remove Access:*** Used to revoke access to the specified application for the person you are reviewing. If revoked and later determined they need access, a new access form for that application will need to be submitted.

Application Roles: To identify the roles an individual has for a specific application, select the checkmark to the left of application in the "My Applications" section (will only apply to applications handled through the Security Model).

Section 5: Automated Security Maintenance

Termination/Transfer Jobs

The termination/transfer jobs will run daily around 6:00AM.

Termination: Indicates user does not have any active/primary appointment. Users access will be revoked.

Transfer: There are four different scenarios:

- ✓ ***Transfer1:*** Org Unit didn't change or if change stayed between HealthCare Orgs (03, 65-89 & 93-94) and Position # didn't change – No action taken on person's access.
- ✓ ***Transfer2:*** Org Unit changed or if change was not between HealthCare Orgs (03, 65-89 & 93-94) and Position # didn't change – No action taken on person's access.
- ✓ ***Transfer3:*** Org Unit didn't change or if change stayed between HealthCare Orgs (03, 65-89 & 93-94) and Position # changed – Suspend person's access.
- ✓ ***Transfer4:*** Org Unit changed or if change was not between HealthCare Orgs (03, 65-89 & 93-94) and Position # changed – Revoke person's access.

Scenario	Org Unit Changed? [1]	Position # Changed?	Action	Notification Sent To?
Termination	n/a	n/a	Revoke access	AFR
Transfer1	N	N	Access remains	n/a
Transfer2	Y	N	Access remains	AFR
Transfer3	N	Y	Suspend access for 7 days	Business Officer & their Admin Delegate(s), "NEW" Department Admins & their Admin Delegate(s), AFR
Transfer4	Y	Y	Revoke access	AFR

[1] – If Org Unit change from one to another remains within HealthCare Orgs (03, 65-89 & 93-94) this will be treated as a no change.

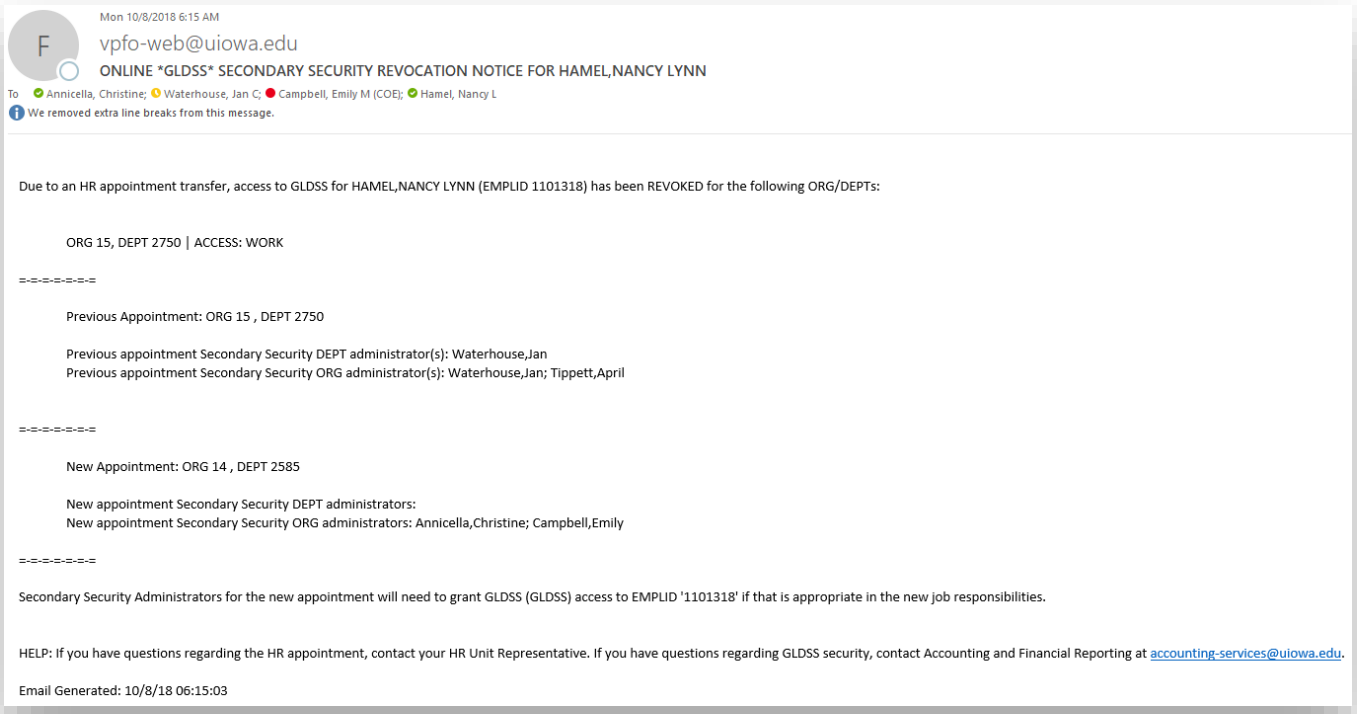
NOTE: Department Admins and their Admin Delegates are not able to reinstate ("unsuspend") in FST. The email is sent so they are aware of staff in their department in a suspended status. They can choose to contact the Business Officer and their Admin Delegates to request access be reinstated or to take no action and access will be revoked.

Security Notifications

Notifications will contain the following information:

- ✓ Employee Name & Employee ID.
- ✓ Identifies that the Position # changed and provides the old and new values (will include Department number & name for reference).
- ✓ Identifies access was suspended.
- ✓ Will provide instruction on what you can do for the person's access
  - Business Officer and their Admin Delegates – Able to reinstate access within 7 days or take no action and access will be fully revoked.
  - Department Admins and their Delegates – Help review access provided in emails and contact Business Officer and their Admin Delegates if access needs reinstated.

Security notification example:



Mon 10/8/2018 6:15 AM

vpfo-web@uiowa.edu

ONLINE *GLDSS* SECONDARY SECURITY REVOCATION NOTICE FOR HAMEL,NANCY LYNN

To Annicella, Christine; Waterhouse, Jan C; Campbell, Emily M (COE); Hamel, Nancy L

We removed extra line breaks from this message.

Due to an HR appointment transfer, access to GLDSS for HAMEL,NANCY LYNN (EMPLID 1101318) has been REVOKED for the following ORG/DEPTs:

ORG 15, DEPT 2750 | ACCESS: WORK

=-=-=-=-=-=-=

Previous Appointment: ORG 15 , DEPT 2750

Previous appointment Secondary Security DEPT administrator(s): Waterhouse,Jan
Previous appointment Secondary Security ORG administrator(s): Waterhouse,Jan; Tippett,April

=-=-=-=-=-=-=

New Appointment: ORG 14 , DEPT 2585

New appointment Secondary Security DEPT administrators:
New appointment Secondary Security ORG administrators: Annicella,Christine; Campbell,Emily

=-=-=-=-=-=-=

Secondary Security Administrators for the new appointment will need to grant GLDSS (GLDSS) access to EMPLID '1101318' if that is appropriate in the new job responsibilities.

HELP: If you have questions regarding the HR appointment, contact your HR Unit Representative. If you have questions regarding GLDSS security, contact Accounting and Financial Reporting at accounting-services@uiowa.edu.

Email Generated: 10/8/18 06:15:03

Section 6: Scenarios/FAQs

Scenario: New Dept Administrator (new external hire)

Assign Dept Admin role(s) in Institutional Roles application.

This would result in:

- ✓ Automatically grants:
  - EFR Access Group
    - EFR Portal (TDR, Admin Reports, Summary Reports, Dashboard, GL Reports & Grant Reports)
    - Financial Systems Tools (FST)
    - Request for GL Chartfields & WhoKeys
    - WhoKey Administration
- ✓ Eligibility to (but requires additional request forms):
  - CumComp
  - Grant DSS
  - EFTx Access Group
    - PayCV
    - WebCV
    - GLJE

Scenario: New Account Reviewer (internal transfer hire)

Assign WhoKey role(s) through WhoKey Administration application.

This would result in:

- ✓ Automatically grants:
  - EFR Access Group
    - EFR Portal (TDR, Admin Reports, Summary Reports, Dashboard, GL Reports & Grant Reports)
    - Financial Systems Tools (FST)
    - Request for GL Chartfields & WhoKeys
    - WhoKey Administration
- ✓ Eligibility to (but requires additional request forms):
  - CumComp

- Grant DSS
- EFTx Access Group
  - PayCV
  - WebCV
  - GLJE

NOTE: While it can be appreciated that one may want to be proactive with granting access for a new hire that will be transferring in, it is not recommended to do this. If this is done, there is the risk that when the transfer is processed that all access will be revoked. This is a known concern and we plan to work on a solution sometime in the future.

Scenario: New Student (new external hire)

Assign GLJE access only through GLJE access request form.

This would result in:

- ✓ Automatically grants:
  - EFTx Access Group
  - EFR Access Group
    - EFR Portal (TDR, Admin Reports, Summary Reports, Dashboard, GL Reports & Grant Reports)
    - Financial Systems Tools (FST)
    - Request for GL Chartfields & WhoKeys
    - WhoKey Administration

Scenario: Employee needs EFR Portal/GL DSS Reports access only but has no WhoKey, Inst. Roles or Transactional application access

Assign Financial Reporting (AFR) only role through ***Financial Reporting (AFR)*** Applications form. The only time this form should be completed is when the user will not be granted access to any of the following financial roles or applications: WhoKey Roles, Institutional Roles, GL Journal Entry, PayCV or WebCV. This restricted form is only accessible to Business Officers to initiate in order to prevent unnecessary requests by campus users when they will automatically be granted this role through another Role or Application access described previously. Business Officers are also the only ones included for Workflow approval and once approved by them, the role is automatically set up.

This would result in:

- ✓ Automatically grants:
  - EFR Access Group
    - EFR Portal (TDR, Admin Reports, Summary Reports, Dashboard, GL Reports & Grant Reports)
    - Financial Systems Tools (FST)
    - Request for GL Chartfields & WhoKeys
    - WhoKey Administration

Section 7: Questions/Contacts

- ✓ GLJE, WebCV & PayCV transactional application questions or related journal searches and All Journal search and CumComp application questions: AFR-ElecFinTrans@uiowa.edu.
- ✓ Security questions: FBIS-DL_Developer-Financials@iowa.uiowa.edu.