

9.2 Offboarding - Security Procedure

Purpose: Use this document as a reference to ensure that an offboarding employee is not active at another institution, and to adjust the employee's roles, SACR and User Preference Definition settings.

Audience: Local Security Administrators

! You must have at least one of these local college managed security roles:

- ZD_DS_QUERY_VIEWER

You must also have each of these roles to run the QHC_SEC_HR_STATUS_SYSTEM_LEVEL query:

- ZD_DS_QRY_SECURITY_TABLES

If you need assistance with the above security roles, please contact your local college supervisor or IT Admin to request role access.

Offboarding - Security Procedure

i When an employee offboards from an institution, it is critical to clean up their security access within the system. It is very important to ensure that the employee is not active at another institution. Since there is only one User ID in the system for an active employee, **it is critical to coordinate with other institutions if the employee transferred and is active.**

It is critical to login to the HCM Pillar and run the query named:
QHC_SEC_HR_STATUS_SYSTEM_LEVEL

This query is meant to serve as a **secondary tool** to help identify inactive employees, vs employees that are still active somewhere in the system. As a security administrator it is important that you also check with your HR counterpart and the HR counterpart at the other institution to confirm employment.

PCD Environment

When offboarding user access, consider the PCD Environment as well. If this is a critical time sensitive offboarding, then the LSA would want to log in to PCD and Lock the account in HCPCD. This will prevent the offboarded employee from accessing Production-like data in PCD. PCD is refreshed monthly, and upon the next refresh the offboarded employee's security access would mirror Production.

1. It is critical to log in to the HCM Pillar and run the query named:
QHC_SEC_HR_STATUS_SYSTEM_LEVEL
2. There is a procedure document for this query named [9.2 Employee HR Status System-wide](#). Please refer to it to decipher the fields and data returned, but the most important two columns are:
 1. **Employee Associated Companies** column will list any companies that the user has ever been associated with. This doesn't reflect active/inactive status, just association over time.
 2. **System Status** will display ACTIVE IN SYSTEM if the person is Active (at one or more institutions across the system), and Inactive in System means that they are **not active at any institution in the system**. The next two columns will show HR Active Company and HR Inactive Companies. If the person is not active at any company the security administrator should clean up the roles/secondary security within each pillar. **If the person is inactive at their institution but active at another, the security administrator should contact the security administrator at the active college and work together to clean up the security for the employee.** From an audit perspective, it is important that the security administrator at the institution the person is leaving, removes any roles (above base employee roles) that they manually added. The new institution's security administrator would then Add back any roles that the person needs to do their job there. There is a record in Query called AUDIT_PSRULEUSER (see queries Qxx_SEC_USER_ROLE_HISTORY and Qxx_SEC_ROLE_EDIT_BY_OPR). This record will show who added/deleted roles from a user. When auditors look at the data for terminated employees, they will be looking to see if the admin at the campus the person terminated performed offboarding. Therefore, it is critical that the roles are removed by that campus. There can be timing issues, especially if HR doesn't enter the termination data in a timely manner. We will be updating the [Onboarding](#) document as well for this procedure. It is a two part effort and has to be coordinated between the colleges.
3. Example: Person Terminates from College A and goes to College B
 1. Steps:
 1. College A should run the system status query to see the person went to College B;
 2. College A's local security admin should contact College B's local security admin and setup a time for offboarding. College A will need to remove any role above base employee access that they assigned to the user, even if the user needs it at college B.

3. Then College B can onboard the employee for their institution so that from an audit perspective it is clear they were Offboarded and Onboarded Properly.
4. Since sometimes there is a timing issue, when onboarding a new hire, it is critical that colleges still run the QHC_SEC_HR_STATUS_SYSTEM_LEVEL query to see if the person was at another institution. They should reach out to the prior institution to repeat the above steps prior to onboarding so that the users access is clean.
5. Once it is confirmed that the employee is no longer active at any institution, follow the below procedures for offboarding by pillar. If they are active at other institutions, you will still need to clean up things like SACR, User preferences etc and coordinate with the other colleges on role removals. See below sections for that as well.
6. The query QXX_SEC_USER_ROLES_NOT_LOCAL should be run in all pillars to show what roles the user has that are NOT on the local role grant list. A ticket should be opened to SBCTC for the security team there to remove these roles for you upon termination. The ticket should contain the appropriate approvals.

HCM Pillar

Regarding Returning Employees

The Local Security Administrator must add the ZZ PeopleSoft User role manually if the person is not new to the system, but is returning as an employee.

When a brand new user profile is created in ctcLink, by default the employee will have the base roles assigned, including the ZZ PeopleSoft User role.

If the employee already existed in the system then left, the ZZ PeopleSoft User role would have been removed as part of Offboarding, When the employee returns to active employment, the role will need to be manually assigned by the Local Security Administrator.

4. When offboarding an employee, the security role of ZZ PeopleSoft User will need to be removed manually by the Local Security Administrator. The security role of ZZ Former Employee will be added dynamically. It is important to make sure the following roles are attached to a former employee so the employee can still access tax information, update their personal details, view old paychecks, etc.
 1. EOPP_USER
 2. PAPP_USER
 3. NA Payroll WH Form User
 4. CTC_%_DISTR (Dynamic)
 5. ZZ FORMER EMPLOYEE (Dynamic)
5. HCM is pretty straight forward as there are no secondary security setups.

Legacy Applications

- If applicable, remove the ZZ LegacyLink role from the HCM Distributed User Profile
- If applicable, remove the ZZ Legacy Transcripts role from the HCM Distributed User Profile
- If applicable, inactivate the user from LegacyLink and/or Legacy Transcripts. See QRG "[Legacy Applications Security Administration](#)".

What can a former employee expect to see and do in ctcLink?

A former employee can expect to see the Employee Self Service tile, from which the former employee can select the Payroll tile or the Personal Details tile.

For former employees, the Process Profile permission, Row and Primary Permissions on the General tab of the Distributed User profile are Not required for them to access their data.

Finance Pillar

6. **User Roles:** Once HCM pillar is updated, then roles will update in Finance. The ZZ PeopleSoft User role will automatically be removed and the ZZ Former Employee role will sync to Financials. There should be no need for a former employee to access Financials, unless they have an outstanding cash advance or expense report, in which case they could work with the Expenses Administrator on their campus to finalize those transactions on behalf of the employee. If the user is active at another institution, please check all workflow type roles and remove your institution route controls from them, as they would still receive workflow transactions if this is not cleared. In Financials, the only roles that should remain are:
1. EOPP_USER
 2. PAPP_USER
 3. ZZ FORMER EMPLOYEE
 4. (CTC_%_DISTR) can be there; this is optional as it only controls Tile access in Portal to your institution. They will retain it in HCM, however there is no harm in keeping it in Finance.

 Finance has secondary security considerations.

7. **User Preferences:** NavBar > Navigator > Setup Financials Supply Chain > Common Definitions > User Preferences > Define User Preferences

- Note: This is Tabs 1-11 on the BI Publisher Report: **BFS_SEC_OPDF**
- **Roles:** ZZ Local Security Admin, ZD Local Security Admin
- It is a good idea to go through all of the User Preferences settings and remove your institution specific Business Unit, especially on the Overall Preferences link, and the Procurement links. In the Requisition and PO Authorization screens, uncheck the allowed actions and clear the Empl ID in the User Auth For field. In the Supplier Processing Authority screen - uncheck the Authority to Enter box. The following reports will assist with identifying existing setup:
 - *User Preferences Report* NavBar>Navigator>Set Up Financials/Supply Chain>Common Definitions>User Preferences>User Preferences Report displays any user preferences by user id. Ensure you select All Products and enter the user id of the terminated user.
 - There is also a BI Publisher report, **BFS_SEC_OPDF**, that can be used for offboarding an employee that captures the Finance Operator defaults & other module-based security assigned to a user in the business unit.
 - NavBar>Navigator>Reporting Tools>BI Publisher>Query Report Scheduler
 - To run the report: Add a new Run Control ID for the BFS_SEC_OPDF report, choose Data Source Type "Connected Query", input report name and template ID as shown. Use the Update Parameters hyperlink to change the GL Unit and User OprID (aka Empl ID) information as needed:

The screenshot displays the 'Query Report Scheduler' interface. At the top, it shows 'Run Control ID: BFS_SEC_OPDF' and 'Language: English'. The 'Report Definition' section includes 'Data Source Type: Connected Query', 'Report Name: BFS_SEC_OPDF', and 'Template ID: BFS_SEC_OPDF_1'. A red box highlights the 'Update Parameters' link, with a red arrow pointing to a modal dialog box. The dialog box is titled 'Prompt for Query CQFS_SEC_OPR_DEF_RPT_CP' and contains input fields for '*GL Unit' (with value WA110) and 'User OprID' (with value 10101). Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog.

Query Name	Prompt Name	Prompt Value
1 CQFS_SEC_OPR_DEF_RPT_CP	BUSINESS_UNIT_GL	WA110
2 CQFS_SEC_OPR_DEF_RPT_CP	OPRID	10101

8. Requester or Buyer Settings:

- User Preferences>Procurement - If the terminated user was a Buyer or Requester in the Purchasing module, navigate to the Procurement page and clear the user's Requester and Buyer fields.
 - Note: This is Tab 12 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Requesters: Click on the Requisition Authorizations link to clear values in the Requester Authorized For section. Unselect the Full Authority for All Requesters if selected.

- Buyers: Click on the Purchase Order Authorizations link to clear values in the Buyer Authorized For section. Unselect the Full Authority for All Buyers if selected.
 - Requester or Buyer Setup: NavBar>Navigator>Setup Financials Supply Chain>Product Related>Procurement Options>Purchasing>Requester Setup or Buyer Setup.
 - IF the user has in-process transactions, it is not advised to inactivate their Requester/ Buyer setup because inactivating their profile could cause issues processing active requisitions or purchase orders.
9. **Grants Security:** NavBar>Navigator>Set Up Financials/Supply Chain>Security>Grants Security
- Note: This is Tab 13 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZD Local Security Admin, ZZ Local Security Admin
 - If the user has access to grant proposals based on Tree SetID and departments, remove this setting by deleting the record (minus sign).

 Finance module-specific secondary security considerations. These settings may be managed by accounting managers for each module.

10. **Department Approvers:** NavBar > Navigator>Setup Financials Supply Chain>Common Definitions>Design Chartfields>Define Values>Chartfield Values
- Note: This is Tab 17 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZD GL Local Config Inquiry, ZZ GL Local Configuration, ZD Local Security Admin
 - If the terminated user was a manager of a department, the Manager ID in the chartfield value setup needs to be updated with the User ID of their replacement; This is critical for some of the workflow routings.

 *****If you are not entering a new effective date, you will need correct history and only the Central SBCTC team has access to correct history, so a ticket will be needed to coordinate the manager update on the chartfields.***

11. **Financial Gateway/Treasury Security:** NavBar > Navigator >Financials Gateway > Security > Security User Assignment
- Note: This is Tab 15 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZD Treasury Local Config Inq, ZZ Treasury Local Config, ZD Local Security Admin
 - If the terminated user had Financial Gateway access, remove the Payment Security Rule (minus sign).
12. **Commitment Control Budget Rules:** NavBar > Navigator > Commitment Control > Define Budget Security > Assign Rule to User id
- Note: This is Tab 14 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZD CC Local Config Inq, ZZ CC Local Config, ZD Local Security Admin
 - If a user had the ability to override a budget date or exception, then you will need to remove the budget security rules upon termination (minus sign).

13. **Procurement Card Proxy:** NavBar>Navigator>Purchasing> Procurement Cards>Security>Assign Proxies
 - Note: This is Tab 19 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZD Purchasing Local Cnfig Inq, ZZ Purchasing Local Config & ZD Local Security Admin
 - If the user is assigned as a proxy (pcard administrator, reconciler, approver, or reviewer), reassign as needed.
14. **Authorize Expense User:** NavBar>Navigator>Travel and Expenses>Manage Expenses Security>Authorize Expense Users
 - Note: This is Tab 20 on the BI Publisher Report: **BFS_SEC_OPDF**
 - Roles: ZZ Expenses User Admin & ZD Local Security Admin
 - Remove additionally added authorized expense users.
 - The query **QFS_SEC_EX_EE_AUTH_OPRID** lists Authorized Expense Users by Business Unit and optionally by Empl ID. This query can be used by Travel & Expense administrators to review and manage Authorized Expense Users assigned to employees at their location.
15. **Travel & Expenses Profile>Organizational Data tab:** NavBar>Navigator>Travel And Expenses>Manage Employee Information>Update Profile>Organizational Data tab
 - Roles: ZZ Expenses User Admin & ZD Local Security Admin
 - Verify that the default profile is in terminated status. If the employee has additional job records that are in active status, the default profile could be changed to the job record that is active. (PeopleSoft requires that at least one job record be checked as default profile.).
 - To add, the default profile checkbox is required to be checked in one of the profiles before saving. It cannot be left unchecked, unfortunately. While offboarding, if new HCM job data has not integrated to FSCM for a new position/college yet, there would be a timing issue. In this case, it may be helpful to let the LSA who is onboarding to check their college as the Default Profile box during their process – or to revisit the page later to update the selection. See QRG [Editing Employee Organizational Data](#) for more information.
 - You must uncheck the default profile checkbox on the Update Profile for Expenses when a person leaves.
16. **Travel & Expenses>Approver Assignment:** NavBar>Navigator>Setup Financials Supply Chain>Product Related>Expenses>Management, Approval Setup>Approver Assignments
 - Note: This is Tab 18 on the BI Publisher Report: **BFS_SEC_OPDF**
 - **Roles:** ZZ Expenses Local Config, ZD Expenses Local Config Inq, ZD Local Security Admin
 - If the terminated employee was a Travel & Expense approver, replace their user id with the user id of the replacement.

Campus Solutions Pillar

17. There is no real need for a terminated employee to have Access to Campus Solutions upon Termination. Therefore, all roles could be removed. However, the administrator must ensure that the employee is not a current or former student. If they are or have been a student they will need to retain the CTC_%_CC role for the college as well as the ZZ SS

Student, EOPP_USER and PAPP_USER roles. For students, we need to LEAVE the row/primary; so if we are offboarding employees, and they are also students, do not remove the row/primary permission list from them in CS. Student access is controlled dynamically by the processes that run in the background that assign the **ZZ SS Student** role. This role is never removed by the LSA, as it is controlled by the system based on the student's engagement at their various institutions. The ZZ SS Student role would be all that is needed for a student. However, having the ZZ Peoplesoft User role wouldn't hurt anything AT all. We did this, because students that were employees, were getting the ZZ PeopleSoft User role removed in HR when they were offboarded. That was also removing it from CS, and preventing users from logging in. So to mitigate that for students, we just added the sign in rights directly to the Student role.

18. **Faculty/Advisor**, whether full or part time, their **ZZ SS Faculty** and **ZZ SS Advisor** roles are assigned dynamically by the existence of an 'active' record for your institution on the Instructor/Advisor table. LSAs *would not manually remove* these roles as the system will only remove these roles if ALL instructor/advisor entries are inactive for all colleges. If a Faculty/Advisor is no longer active at your institution, it is recommended to inactivate them on the instructor advisor table. Mark the row 'inactive' and do not delete. Deleting the row can cause the advising notes on a student to not be visible. Visit the QRG [9.2 Inactivate Instructors at Multiple Institutions](#).
19. SACR Values should be cleared for your institution if they are not a student there: **NavBar > Navigator > Setup SACR > Security > Secure Student Administration > User ID, Roles:** ZD Local Security Admin, ZZ Local SACR Security Admin
20. Clear all institution values from here for your college: **NavBar > Navigator > Setup SACR > Security > Secure Student Financials > User ID, Roles:** ZD Local Security Admin, ZZ Local SACR Security Admin
21. If you add a user to the Access Control tab of the Note Category Table, upon termination this needs to be removed: **NavBar > Navigator > Setup SACR > Product Related > Academic Advisement > Note Category Table, Roles:** ZC SACR AA Config, ZD CS ADVISEMENT SETUP, ZD SACR Advisement Config
22. If the employee is not a student and not active at another college you could use the User Security Replacement tool, to pull up the employee and copy from a userid that doesn't have **ANY SACR** values to wipe it out. Visit the QRG [9.2 SACR Security - User Replacement Security \(Onboarding/Offboarding\)](#).
23. There is a BI Publisher Report that can be run to identify SACR for an individual: BCS_SEC_SACR ; Run this to identify what SACR a person has. Please refer to this QRG for run instructions: [9.2 Run the BCS_SEC_SACR Report](#).

RED ALERT! & How to Kick a User Off of ctcLink Immediately!

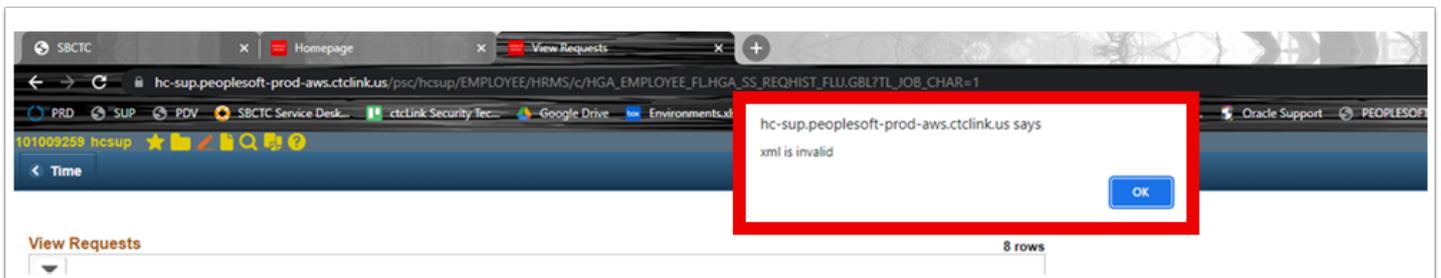
 Here's the quickest way to terminate a logged-on ctcLink user's access.

1. In the Distributed User Profiles "Roles" tab, remove the ZZ PeopleSoft User and ZZ SS Student roles.

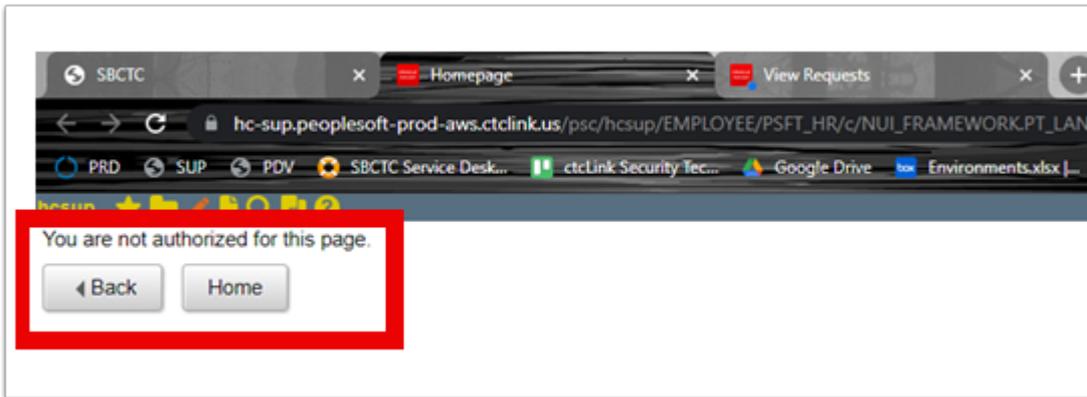
2. In the Distributed User Profiles "General" tab, check the **Account Locked Out?** checkbox.
3. Select the **Save** button.

The screenshot shows the 'Distributed User Profile' page in 'Employee Self Service'. The 'General' tab is active. The 'User ID' is 10100. The 'Account Locked Out?' checkbox is checked and highlighted with a red box. Below this, there are sections for 'Logon Information' (Symbolic ID: SYSADM1, Change Password?, Password Expired?, User ID Alias), 'General Attributes' (Language: English, Currency, Default Mobile Page, Enable Expert Entry), and 'Permission Lists' (Navigator Homepage, Process Profile, Primary, Row Security). At the bottom, the 'Save' button is highlighted with a red box, along with 'Return to Search', 'Add', and 'Update/Display' buttons.

4. The next time the user selects something, the selection will fail and the following error message will display:



5. The next time the user tries to launch into a pillar from the main landing page, the following error message will display:



6. Now that the user is no longer able to access ctLink, the offboarding process can proceed:
 1. Local Security Administrator completes offboarding as described in the other sections of this QRG.
 2. Human Resources completes termination in HCM pillar per college procedures.
 3. Local Security Administrator unchecks the Account Locked Out? checkbox to give the terminated user access to ctLink as a former employee and/or a former student
7. Section complete.

Additional SBCTC Systems with Offboarding Implications

Below are the applications where user access is managed by **Data Services** that should be included in the college offboarding process

- **QARS** - Quality Assurance Reporting System A web-based application used to provide the colleges with data issues that impact the data warehouse and that need resolved before we take the snapshot. It also includes some other reports that are not data warehouse dependent such as for HCM IPEDS reporting. But the primary usage is to provide info back to the colleges on data issues we are finding that need cleaned up before the end of quarter snapshot. **To include: ctLink TicklerSERS ---Accounts are currently managed by Data Services staff and we would like to be informed when a user's access should be removed via ticket.**
- **Tickler** - A web-based application used to remind the colleges of the dates we are taking snapshots for the data warehouse. Other teams may be using the Tickler as well, but I'm only familiar with the Data Services use of the tool. **Accounts are currently managed by Data Services staff and we would like to be informed when a user's access should be removed via ticket.**
- **metaLink** - A web-based application used to deliver a data dictionary for each of the ctLink tables. The data dictionary access requires a username and login. There is also a public page in metaLink used to search for queries and other reporting objects using key words, but this part does not require a username and password so no offboarding needed. **Accounts are**

currently managed by Data Services staff and we would like to be informed when a user's access should be removed via ticket.

- **dataLink** - An Oracle database that contains the ctcLink replicated college specific ctcLink data. **Database user accounts are currently managed by Data Services staff and we would like to be informed when a user's access should be removed via ticket.**
 - dataLink access requires not only a named user account in the database, but is also associated with the person's IP address at the college. If the user tries to connect to dataLink from their personal device, the access will be denied. Kenn's network team may want to be included so that they can remove the IP access.
- **WABERS** - Washington Basic Education Reporting System A web-based application used to collect information related to students taking adult basic education classes. **User access is managed by the college.**
- **Solar Winds** - Ticket System There is a list of clients that have access to the ticket system. **To be removed, a ticket to SBCTC should be submitted.**
- **HP3000 (HPUX) Legacy data** - **System admin at colleges have access to update.**
- **Online Transcript Legacy data** - **Local Colleges have access to administer this.**
- **WCTCS Portal (Legacy Web Admissions)** - **Local Colleges have access to administer this.**
- **Canvas access** - Access to our project and training courses **Colleges are responsible for creating accounts and offboarding the accounts. If a staff member has access to multiple Canvas Accounts, and things need to be merged, a ticket to SBCTC is needed.**
- **Email ListServ** - Depends on listserv
- **CyberSource** - Colleges are responsible for managing their own CyberSource users.
- **NelNet**
- **25Live/LYNX** - Academic and Event Scheduling program - **Access to this program is managed by the schools with technical and functional support provide by SBCTC.** LYNX is an "interface placed between 25Live and Campus Solutions that is used to import and export academic data (and keep in sync) between the two systems." **Access to this interface is managed by SBCTC with technical and functional support provided by SBCTC.**
- **Online Admissions Application Portal (OAAP)** - **For OAAP a ticket to SBCTC needs to be entered to request the user be removed from the admin portal**
- **CampusCE** - **The college needs to notify and work with CampusCE to have any staff accounts in CampusCE deactivated.**
- **Tableau** - **Colleges Manage Locally?**
- **Oracle Support Accounts** - **Colleges Manage Locally.**
- **ctcLink TicklerSERS**

Process complete.

Video Tutorial

The video below demonstrates the process actions described in steps listed above. There is no audio included with this video. Select the play button to start the video.

Video Tutorial via Panopto

View the external link to [Offboarding Security Procedure](#). This link will open in a new tab/window.