Employee Offboarding Guidelines & Checklist

Information resources, including data created and used by the California State University System (CSU) and Cal Poly Pomona (CPP), are critical assets of the CSU and Cal Poly Pomona.

It is the policy of the CSU that access to information resources is removed at the end of employment, or when job duties no longer provide a legitimate business reason for access. When an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked. Information assets accessed by the employee need to be properly disposed or transferred upon termination. (ICSUAM 8000)

Risks & Considerations

Campuses must ensure that their information assets and services can continue to operate and be appropriately accessible to users through and after disruptions, which includes employee separations. This includes ensuring the continuity of essential functions and operations. (ICSUAM 8000)

Employee Offboarding Guidelines

1. Paper files must be promptly reviewed by the appropriate manager to determine if the files require retention. If the files require retention, the appropriate manager will determine who will become the data steward of such files and transfer the files accordingly.
2. Access to electronic files must be promptly reviewed by the appropriate manager to determine if others require comparable access or the files need to be transferred to ensure continued operations, as well as appropriate data retention. Employees can obtain incidental personal electronic information as appropriate.
3. Access to electronic applications and systems must be promptly reviewed by the appropriate manager to determine if others require comparable access to ensure continued operations.
4. Physical access should be reviewed by the appropriate manager to determine if access should be transferred to another staff member to ensure continued operations.
    - Items granting physical access such as keys and access cards must be collected from the exiting employee. Any access list that grants the exiting employee physical access to a limited-access area on the campus must be updated appropriately to reflect the change in employment status.
5. Telephone assignments must be reviewed by the appropriate manager to determine if assignments should be forwarded and/or reassigned.

Any exceptions must be documented by the campus Chief Information Security Officer (CISO) and authorized by the division Vice President and Chief Information Officer (CIO).

Manager & Employee Offboarding Check List

1. **Computing equipment** – computer, tablets, hotspots, monitors, etc.
   - □ The employee's department Dean/Director or Department Head and employee signs the *HR Operations Clearance Form* to indicate that the employee has returned any desktop or mobile computing equipment assigned.
     - ✓ Contact the IT Service Desk for IT&IP Client Services to obtain a list of equipment assigned to an employee.
     - ✓ Contact the IT Service Desk for IT&IP Client Services to schedule assistance with receiving equipment from the employee.
2. **Email**
   - □ Determine if the employee's email address should forward messages to another email address, and for what period.
     - ✓ Employee can set this up within their email account prior to separation. Contact the IT Service Desk for assistance.
   - □ Establish an Out of office message for the separating employee's email address.
     - ✓ Employee can set this up within their email account prior to separation. Contact the IT Service Desk for assistance.
     - ✓ If you are requesting direct access to an email account beyond forwarding, a request from the area AVP needs to be sent to the campus CISO. The CISO can be reached at CISO@cpp.edu.
3. **Phone extension and Voice Mail**
   - □ Determine if the employee's phone extension should have an out-of-office message and/or be forwarded to another campus extension.
     - ✓ The employee can set this up in their voice mail prior to separation. Contact the IT Service Desk for assistance.
4. **PeopleSoft or other Enterprise System Access** using Bronco Credentials (Single Sign On)
   - □ Review PeopleSoft and other enterprise system access with the employee to determine if access needs to be provided to someone else prior to separation.
     - ✓ The HEERA manager can contact the IT Service Desk to request IT&IP for a list of PeopleSoft or other system access assigned to the employee for the manager to review. Requests need to be made by the HEERA manager or higher-level manager, and then reviewed/approved by the CISO. The campus CISO can be contacted via CISO@cpp.edu.
5. **Application Access** NOT using Bronco Credentials (non-single sign-on)
   - □ Review and remove access to applications that do not use Bronco Credentials.
     - ✓ Contact the application administrators of those applications to obtain a list of permissions and remove access.
   - □ If employee is an application administrator, transfer administrative privileged/administrative access to another employee with the appropriate knowledge, skills, and abilities.
     - ✓ Contact campus Chief Information Officer (CIO), Deputy CIO, or CISO for questions or assistance. The campus CISO can be contacted via CISO@cpp.edu.
6. **Department File Shares, Microsoft Teams and SharePoint**
   - □ Review access and determine if any permissions, roles/responsibilities need to be provided to someone else prior to separation.
     - ✓ Contact the IT Service Desk to request IT&IP for a list of Identity Management Group and Microsoft group/team memberships assigned to an employee for manager review. Requests need to be made by the HEERA manager and will be reviewed/approved by the campus CISO.

7. **Permission Groups or Moderated Email Lists**
   - □ Review and transfer any permissions, roles/responsibilities for groups and email lists.
     - ✓ Contact the IT Service Desk to request IT&IP for a list of Identity Management permissions groups or moderated lists where the employee may be an owner. Requests need to be made by the HEERA manager and will be reviewed/approved by the CISO.
8. **One Drive Files** - Every employee is provided an Office 365 One Drive account. For computers provisioned by IT&IP, the computers are configured to replicate the Document folders to One Drive for business continuity purposes.
   - □ Review the files with the employee to determine which files need to be retained and transferred to a department file share so that others can access the files after the employee separates.
9. **Social Media**
   - □ Review and transfer any roles/responsibilities employee has for campus social media accounts. This can include administrative access, communication posts, responses, etc.
   - □ Transfer any administrator access accounts to another employee for campus social media accounts.
10. **Paper files**
    - □ Review paper files to determine if the files require retention.
    - □ Transfer paper files requiring retention to another employee for retention and data stewardship.
11. **Door Access**
    - □ Review door access to determine if other employees need comparable access to open or close doors.
12. **Other Items**
    - □ The *HR Operations Clearance Form* includes information regarding other items that should be returned by the employee to the employee's department Dean/Director or Department Head, including keys, credit card, library materials, and parking decal.
    - □ The employee's department Dean/Director or Department Head will return the collected items as directed by HR.
13. **Emeritus status** is granted annually in November. However, employees can be provided pending emeritus status by HR during the "gap" period, the period between the point of retirement until the formal emeritus status is granted in November. This is provided on an exception basis, upon request from the employee/retiree to their respective HR department who may facilitate the appropriate approvals with the employee's department manager, etc. This typically occurs in situations where the retiree would like access to their CPP email while they wait for emeritus status to be formally granted by the University.
    - ✓ Account Access will be temporarily discontinued while the employee is formally separated from the University, and their employee-related access is removed.
    - ✓ Access is enabled by IT&IP once the emeritus status is granted and IT&IP has reviewed that employee permissions have been removed.
    - ✓ For more information regarding the campus emeritus award and related privileges, refer to https://www.cpp.edu/president/honoring-exellence/emeritus-awards.shtml

SIGNATURES

The signatures below indicate that the employee and HEERA manager have reviewed the employee offboarding checklist items.

If access to employee's electronic account information, such as email, files, is required after separation, the employee, HEERA, AVP, or Vice President should contact the campus CISO at ciso@cpp.edu. All requests are subject to CISO and CIO review and approval.

Employee Signature:

______________________________	______________________________
Name (Please print)	Signature
______________________________	______________________________
Title	Date

HEERA Manager:

______________________________	______________________________
Name (Please print)	Signature
______________________________	______________________________
Title	Date

Comments

____

____

____

____

____