CHECKLIST for INFORMATION SYSTEMS ACCESS

For INVOLUNTARY SEPARATIONS

PLEASE CONTACT INFORMATION SECURITY ***PRIOR*** TO THE SEPARATION MEETING

Due to the potential risks the institution carries when a terminated employee retains any access rights to campus systems, we strongly advise that all accounts are locked ***during*** the termination meeting. Please coordinate this timing in advance with Information Security (Josh Callahan, x3815). If the appropriate administrator decides to accept the risk of maintaining some access for the terminated employee, use the following checklist to determine which accounts are retained.

Employee Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Separation Date: \_\_\_\_\_\_\_\_\_\_

**Account Checklist**

|  |  |  |
| --- | --- | --- |
| **Account Group** | **What it gets you access to** | **Delete or retain until** |
| PeopleSoft HCM | Human resources or student systems/data (does not turn off access to self-service; see LDAP below)  | Delete **\_\_\_\_\_\_\_** |
| PeopleSoft CFS | University financial data | Delete **\_\_\_\_\_\_\_** |
| Google Apps | Campus email, calendaring, collaborative files | Delete **\_\_\_\_\_\_\_** |
| LDAP | Required for all the above plus PeopleSoft self-service and single sign-on applications (those apps available through myHumboldt portal) | Delete **\_\_\_\_\_\_\_** |
| Active Directory | Desktop computers, network file shares, remote access to campus services, secure wireless  | Delete **\_\_\_\_\_\_\_** |

I understand that the potential risks of retaining access for terminated employees include:

* Continued access to campus protected data
* Employee could claim to still represent the campus to vendors, colleagues, or students via email
* Employee could receive sensitive information by continuing to be on distribution lists after termination

Appropriate Administrator: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**HSU Policy clarification regarding Involuntary Separation**

Involuntary separation of employees will result in immediate termination of access to campus information systems unless otherwise explicitly authorized in writing by the employee’s appropriate administrator, irrespective of an active employee record existing in PeopleSoft solely for the purpose of delivering three additional months of pay.

The university is required by system-wide policy to promptly revoke all access “upon termination of employment, or when job duties no longer provide a legitimate business reason for access” (ICSUAM 8030).  Further, as stated in the CSU Responsible Use Policy (ICSUAM 8105), university information assets are provided to facilitate a person’s role within the university.

Detailed references:

As stated in Title 5, §42723:

1. Except in the case of layoff, the President or Chancellor, as appropriate, shall give a MPP employee, with the exception of athletic personnel appointed to definite terms under (b) above, notice of termination at least three months prior to the employee's separation date or shall give a MPP employee, with the exception of athletic personnel appointed to definite terms under (b) above, corresponding salary in lieu of notice.

CSU Information Security Policy <http://www.calstate.edu/icsuam/sections/8000/8030.0.shtml>

Campuses must implement procedures to revoke access to information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy and by the data owner.  Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the campus, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

CSU Responsible use policy http://www.calstate.edu/icsuam/sections/8000/8105.0.shtml

4.5.1 University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.