Procedure for Employee Separation
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Published</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>10/08/2008</td>
<td>Doug Markiewicz</td>
<td>Original publication</td>
</tr>
</tbody>
</table>
Purpose

The purpose of this Procedure is to provide step-by-step instructions for processing an employee separation with respect to the handling of computing resources. This Procedure is a supplement to the Human Resources Employee Separation Checklist.

Applies To

This Procedure applies to anyone processing the separation of a student worker, faculty or staff.

Procedure for Voluntary Employee Separation

The following are step-by-step instructions for voluntary employee separation.

1. **Process the employee’s separation in HREM**

   While this step is listed in the Human Resources Employee Separation Checklist, it is cross-listed here due to its importance in suspending and removing certain user access. Processing the employee’s separation in HREM should be completed as soon as a separation date is known. A step-by-step guide to completing this can be found in the HREM Reference Manual provided by Human Resources. Following a 21 day waiting period from an employee’s separation date, his or her Andrew account and Microsoft Active Directory account will be automatically suspended. If the employee is registered as a student, the automatic suspension will not occur and manual intervention may be required (see Step 2). Several additional actions are taken automatically, including removal of any network registration entries and revocation of any digital certificates associated with the employee.

2. **Suspend or remove access to systems and applications**

   Employees typically have access to a variety of systems and applications based on their job responsibilities. This access will need to be suspended or removed upon separation. Managers should maintain a list of what systems and applications his or her employees have access to so that it is available when a separation occurs. The types of systems and applications that an employee might have access to include:

   - **Computing Services systems and applications**
     
     As referenced in Step 1, suspension or removal of access to some systems and applications, managed by Computing Services, may occur automatically (e.g. Andrew account access and Microsoft Active Directory account access). Other applications may require manual suspension or removal. Contact the Help Center if you have questions related to suspension or removal of access to system and applications managed by Computing Services.

   - **Department, college or non-Pittsburgh campus systems and applications**
     
     Many systems and applications are managed by a department, college or non-Pittsburgh campus computing staff. If an employee separation occurs within one of these functional areas, the departmental administrator for that area should be contacted to assist with suspension or removal of access. Some functional areas also maintain their own help desk, which can also serve as a resource for suspending or removing access.

   - **Third-party managed applications**
     
     The University outsources a variety of services (e.g. data processing) to third-party providers. Employees are often provisioned user accounts to gain access to these services. The process of
suspending or removing this access will vary from one service to the next. If it is unclear who to contact in order to suspend or remove access to a third-party application, contact either the Computing Services Help Center or your departmental administrator for assistance.

3. **Change any shared account passwords that were known by the employee**

   While typically discouraged, it is often a requirement that multiple users share the password to a single account. For example, the password to a local Administrator account or an application’s super-user account may be shared by more than one employee. If the employee is in possession of one of these shared passwords, it should be immediately changed.

4. **Disable employee’s access to the voicemail system**

   The Telecommunications team within Computing Services is responsible for the University’s voicemail system. There are several alternatives available to address employee separation including changing the employee’s voicemail password, changing the voicemail message to indicate new contact information or simply disconnecting the voicemail. Contact the Telecommunications team by phone at 412-268-8500 to discuss alternatives for disconnecting voicemail. If it is necessary for you to obtain access to a separated employee’s voicemail inbox, please contact the Information Security Office Incident Response team by phone at 412-268-2044, or via email to iso-ir@andrew.cmu.edu.

5. **Revoke physical access to secure facilities and retrieves keys and/or access cards**

   Employees are provided with physical access to facilities in several manners. The Carnegie Mellon ID+ Card provides access to various facilities depending on particular job responsibilities. Computing Services issues secondary access cards to employees who require access to centrally managed computer rooms (e.g. A-84 and A-100 in Cyert Hall). Other departments (e.g. the Parking Office), colleges or campuses may issue their own access cards. Additionally, an employee is likely provided a set of keys to gain access to his or her building, laboratory, office space and/or filing cabinets. Upon separation, all access cards and keys should be collected from the employee and returned to the appropriate coordinator.

6. **Retrieve computing hardware from the employee**

   Upon separation, all computing hardware issued to an employee will need to be collected. This includes but is not limited to any University-issued laptops, desktops, computing peripherals, cell phones and hardware tokens (e.g. RSA SecurID tokens). Any hardware token the employee may have should be immediately returned to the appropriate administrator. All other hardware can be re-used as deemed appropriate by the manager of the employee. In those limited circumstances where ownership of computer equipment is transferred to the separating employee, the following steps should be considered:

   - Archive any business related documents, as directed by the separating employee’s management
   - Remove all non-public information that is owned or licensed by the University
   - Remove all software applications that are licensed by the University
   - Remove all Microsoft Windows operating system upgrades (only the original manufacturer installed operating system should be transferred to the separating employee)
   - If necessary, erase the entire content of the device’s hard drive using tools and techniques outlined in the [Guidelines for Data Sanitization and Disposal](#).
Procedure for Immediate Employee Separation

The following are step-by-step instructions for immediate employee separation. These steps assume that you have already contacted your Human Resources representative and the Office of General Counsel regarding the immediate separation.

1. **Notify the Information Security Office of the employee separation**

   Send an email to the Information Security Office at iso-ir@andrew.cmu.edu and carbon copy both your Human Resources representative (see **HR Staff Contact Information**) and your contact in the Office of General Counsel. The email should specify the following:

   - The separating employee’s name and department
   - All known account names/access that should be suspended
   - The date and time when access should be suspended
   - Whether a bounce message (an automated reply to incoming email) should be applied to the employees’ Andrew email account and, if so, what that message should say (e.g. it may be desirable to direct business correspondence to a different Andrew email address)

   The Information Security Office is also available by phone at 412-268-2044, Monday thru Friday from 8:30 a.m. to 5:30 p.m., but the email request is still required for tracking purposes. During non-business hours, the phone number listed above will provide emergency contact information. Once the Information Security Office confirms the separation with the Office of General Counsel or Human Resources, the following actions will be performed:

   - The employee’s Andrew account will be suspended
   - The employee’s Active Directory account will be suspended
   - The employee’s Kerberos principal will be set to expire
   - Appropriate system administrators will be contacted to request revocation of access to critical systems including but not limited to HRIS, SIS, Oracle Financials, Tartan Trust Card, Advance C/S, Events Management and systems managed by Sponsored Research
   - If requested, a bounce message will be applied to the Andrew e-mail account
   - The need to preserve electronic content in Computing Services’ systems and applications will be determined in consultation with the Office of General Counsel

   The Information Security Office will also be available to discuss alternatives for gaining access to business related materials that may reside in the employee’s Andrew email account, on shared file systems that are managed by Computing Services (e.g. AFS and DFS), on voicemail, or on a computer that the University issued to the employee.

2. **Suspend or remove access to decentralized systems and applications**

   Contact the administrators of any departmental, college, non-Pittsburgh campus, or third-party managed systems and/or applications to immediately suspend the employee’s access.

3. **Follow the Procedure for Voluntary Employee Separation**

   Once user accounts and access rights are suspended, follow the Procedure for Voluntary Employee Separation as described above. Some of these steps may have already been completed as part of the immediate separation; however, they should all be reviewed for completeness.
4. **Contact the Office of General Counsel regarding destruction and/or reallocation of electronic resources**

Prior to conducting any routine data destruction or reallocating electronic resources assigned to the separating employee, contact the Office of General Counsel to discuss any data preservation needs. This includes but is not limited to data stored on central file services (e.g. AFS and DFS), data stored in the separating employee’s email account and data stored on a computer that was allocated to the separating employee.
Additional Information

If you have any questions or comments related to this Procedure, please send email to the University Information Security Office at iso@andrew.cmu.edu.

Additional information can also be found using the following resources:

- Human Resources Employee Separation Checklist
  https://www.cmu.edu/hr/hr_services/forms/SeparationChecklist.pdf

- HREM Reference Manual
  https://www.cmu.edu/ba/hr/forms/HREMRefMan.pdf

- Help Center Contact Information
  http://www.cmu.edu/computing/repair/help-center.html

- Computing Services Telecommunications website
  http://www.cmu.edu/computing/network/phone/

- Guidelines for Data Sanitization and Disposal
  http://www.cmu.edu/iso/governance/guidelines/data-sanitization.html