System Access Removal Checklist

Employee business data (e.g., email, electronic documents, paper documents, etc.) created while employed at NC State University are university property, and the department may retain them for business use.

During a planned separation, employees and managers should follow the recommendations below, in conjunction with the Human Resources - Employee Separation Checklist or Human Resources - Transferring Employee Separation Checklist, as appropriate.

For a sample list of technology resources to be removed from separating employees, see: Sample List of Technology Resources to Process for Separating Employees.

Subject	Description	Employee Initials (or N/A)
Email	Separating employees are responsible for sharing needed emails with their managers, prior to separation, by forwarding important message and carbon copying (Cc) their managers on relevant email communications.	
Email	Separating employees should provide any ongoing correspondences with updated contact information, to continue any active business.	
Email	Separating employees should set up vacation rules for emails that may arrive in their inboxes after they've left, but before their accounts are deactivated (a period which can occur after termination date). For example, a vacation rule might include the following message: "I am no longer with [department.] Please contact [individual] for assistance."	
Email	Separating employees should tag personal email messages with the label "personal."	
Retiree Email Account	Retiring employees may retain their university email accounts. However, the employee's department is required to submit a no-pay personnel action.	
Google Calendar (personal)	Separating employee should review their personal calendar for any past or future meetings, events, or other information that a manager or coworker might need to access after the employee has left.	
Google Calendar (personal)	Separating employees may wish to change the ownership of single calendar appointments by clicking on a calendar event and choosing "Change Owner" from the More Actions list at the top of the page. The owner can be changed to a sub-calendar and another person.	
Google Calendar (personal)	Separating employees can export their entire personal calendars into an .ics (iCalendar) file for their manager to import into the manager's own calendar. NOTE: Employees should first cancel all future scheduled business meetings that include their manager, prior to exporting, so as not to create duplicate meeting entries when the manager imports the calendar.	

System Access Removal Checklist

Subject	Description	Employee Initials (or N/A)
Google Sub-calendar(s)	Separating employees should follow the process to share an existing calendar, in order transfer the Manage and Share permissions for business sub-calendars that they created to other individuals.	
Google Sub-calendar(s)	Separating employees can export their entire sub-calendar(s) into .ics (iCalendar) file(s) for their manager to import into another calendar.	
Files on home/personal equipment	Separating employees should download any university-related documents that are stored on any personally-owned computers/devices or accounts and grant access to the department, before leaving. These documents should be downloaded to and stored on university-owned resources.	
Application software on home/personal equipment	Separating employees must remove any university-owned software from personally-owned computers or devices.	
Personally-owned devices	Separating employees who have used any personally-owned mobile computer or device (such as a laptop, tablet, or smartphone) for university business must ensure any and all university data are extracted and preserved on appropriate university resources. NOTE: If the device is personally-owned, then it should not be wiped clean without the separating employee's permission.	
University-owned devices	University-owned devices should be wiped clean and re-used or surplussed, as appropriate.	
Voicemail	At the commencement of the separation transition, a separating employee should change his or her voicemail access code(s) and give the code(s) to his or her manager.	
Google Docs/Drive	Separating employees should transfer any Google Docs/Drive important or needed business documents to their manager. First, follow the process to share with specific people (if it is not already shared). Then, follow the process to change the owner of a file or folder to the manager. NOTE: The process described above will also work for Google Forms and Google Sites.	
Google Apps for Education Account Data	Separating employees may download backup copies of their photos (Picasa), profile information, contacts, circles, stream posts and Buzz posts prior to leaving, if they so choose: https://takeout.google.com/settings/takeout.	

System Access Removal Checklist

Subject	Description	Employee Initials (or N/A)
Local and Network Drive Files	Separation employees should identify any files on local or network drives that the employee administers or can access and should transfer ownership of files to departmental shared space, as directed by management.	
Encrypted Business Data and Keys	Upon notification of an employee's separation, his or her manager should find out whether the employee uses encryption on any of their computer devices. If the employee is using personal keys to encrypt the data, the employee should provide all requested business data to the manager. If the separating employee uses business encryption keys, then their manager should obtain encryption keys and associated passwords or pins. The password or pin may be changed by the employee, before it is provided. The manager should also change the password, after the employee leaves. • Having a key escrow system in place for disaster recovery is useful and may eliminate the need to perform these tasks when an employee is leaving. • Most of our university full-disk systems should have key escrow that can be used to obtain the encryption pin. • Encryption keys or pins should always be transferred using secure methods that are appropriate for storing the keys.	
Public Records	Managers should make sure appropriate public record copies of documents from separating employees exist.	
Access to Systems, Accounts, Applications, and Resources	Managers should identify a separating employee's' access to department-owned systems, Web space, or shared accounts, such as Google generic accounts. • Managers should suspend or remove access, as appropriate, and change passwords on the employee's separation date. • Changes should be in effect the day after the separation date. • In addition, managers should identify any resources that the employee administers, transfer administration appropriately, and change any associated passwords. ○ Resources that separating employees either own or administer may include, but are not limited to: shared mailboxes, conference rooms, projectors, and other items owned in Web Registry, such as Global Resources or Google groups.	

System Access Removal Checklist

Subject	Description	Employee Initials (or N/A)
External accounts, including Cloud storage other than Google	• If the separating employee has external accounts used for university business, those should be documented, re-assigned and terminated, if appropriate. For example, employees might have accounts with outside vendors to create support tickets or exchange data with another institution or business partner, on behalf of the department or university. • Further, separating employees may be using Cloud storage tools, such as DropBox or iCloud, for university business. As part of this step, the employee or manager should designate another individual to take over responsibility and create an account for that person, if necessary, to maintain continuity.	
Email lists or Groups	• Managers should identify the employee's administration of any departmental email lists, groups or any use of individual email aliases as a departmental alias. • Administration and use should be transferred appropriately, and any associated passwords should be changed. For example, employees may have established an email list such as "committeeX@lists.ncsu.edu" or a Google group called "CommitteeY" to facilitate communications to members of a particular committee.	
Enterprise Systems managed by SAR (System Access Request)	• The department's SAR administrator should submit a SAR revoke action to suspend access to enterprise applications, such as HR, SIS, Financials, and Web Leave, in a timely manner. • The request should be submitted in advance of an employee termination notification with an effective date, so that the action is invoked at the appropriate time. • There are options for making the request effective immediately (default) or at a future date. • This process automatically allows separated employees to access appropriate self-service roles (e.g., W2 information) through the end of April of the year following their departure from the university. • Access SAR via MyPack Portal. Choose "For Faculty & Staff" → "Security Access/SAR" (left side) → "SAR."	
Other system access	Managers should identify the employee's access to any other systems (e.g., MySoft, Proteus, Facilities), remove access, and change passwords accordingly, in a timely manner.	