

**Policy**

**Employee Termination: Information Access and Resource Disposition**

**Purpose:** The purpose of this policy is to address actions taken regarding the electronic access and disposition of resources associated with an employee at the time of their termination from Claremont McKenna College.

**Scope:** This policy applies to all employees including faculty and staff employed by Claremont McKenna College who have been granted any computing/network access during their employment.

<b>Definitions:</b>	<b>Term</b>	<b>Definition</b>
	Involuntary or not in good-will termination	Usually involves little or no notice on the part of the employee and/or the supervisor/manager, under circumstances that warrant prudent measures to protect the business interests of the college.
	Voluntary or good-will termination	When an employee initiates the separation and/or when there is absolutely no expectation that the employee could be harboring bad feelings that could be manifested in damaging actions in the computer

resources.

**Discussion:** The College does not normally review the content of an employee's electronic communications or data, but these resources are stored on College computer systems and Claremont McKenna College reserves the right to retain and access them as part of its responsibility of maintaining the College's technology infrastructure or when deemed necessary for business purposes. It is important that electronic communications and data can be retained and properly dispositioned at the termination of an employee to protect and preserve as appropriate the information resources of the college. This may involve granting permissions to other employees to become data stewards of the communications and resources previously allocated to a departing employee. The appropriate individual(s) to become the data stewards of a terminated employee's information resources will be determined by the departing individual's supervisor.

**Policy:** In the case of involuntary termination or termination that may be deemed as not in good-will, it is the responsibility of the supervisor or manager of the employee in coordination with HR to establish communications with the Director Information Systems and Network Services (ISNS) preferably prior to or at worst case immediately at the time of termination to mitigate any loss of or damage to informational resources. ISNS staff will immediately alter the terminated employee's password(s) to prevent access. Any access by the employee after termination to information resources will be approved by the terminated employee's manager and facilitated by way of data extraction on physical media (i.e. CD or DVD), which will be made available to the terminated employee if deemed appropriate. Alternately, information may be removed by way of joint review/removal by the terminated employee's supervisor or manager in the presence of the terminated employee if deemed appropriate by the manager. Resources will be dispositioned after termination according to instructions provided by the employee's supervisor on the ITS Termination Checklist, which will be processed as soon as possible after notification.

In the case of voluntary or good-will termination, account access and resources will normally be dispositioned according to instructions provided by the ITS Termination Checklist as defined by the

supervisor of the terminated employee. Accounts are to be modified to deny access by the terminated employee at the end of the day of termination, unless specifically extended or otherwise directed by HR. If an ITS Termination Checklist has not been completed by the supervisor, the ISNS Staff will simply change the password based on HR notification through the help desk system.

**Revisions:** 10/5/05 -Created