ADM 402
Security Policy #2

Termination Policy

Purpose of Policy

This policy defines the steps required to revoke both physical and system access to the College's facilities and network resources.

Termination of Access: it is essential that supervisors and/or Information Technology (IT) terminate access to college facilities and systems in a timely manner to protect the information, systems and resources. Supervisors / IT are required to terminate access immediately upon termination (or even before when possible) of the employee, workforce member or contractor.

1) A terminated employee shall be required to surrender all keys, IDs, access cards/codes or badges, business cards, parking permits and the like, that permit access to The College's premises or information.

2) A terminated employee's physical and electronic access to PII and sensitive college data must be immediately blocked.

3) A terminated employees must return all records containing PII and sensitive college data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

4) Revoke all computer, network, and data access the terminated employee has for both internal and external systems:

    1) Internal systems
        1. Microsoft Windows / Network Domain
        2. Systems that store or access PII and sensitive company data
        3. Email
        4. Database applications
        5. Any other systems that the terminated employee has access to

    2) External systems
        1. Cloud based systems such as credit card processing systems, billing systems, customer relationship management (CRM), etc.

5) Remote access should be removed

6) Wireless access should be removed

All termination steps that are taken should be documented and retained for legal purposes and/or federal or state regulations.