



**POLICY 08:13:12**  
**DATA ACCESS MANAGEMENT**

Access to applications and college information is granted based on an individual's relationship with the College and the individual's job responsibilities. Managing user account access is a continual process and vital to the security of information systems. Only authorized users should be allowed access to grant, review, deactivate, update, and/or terminate account access to information systems.

All systems and files that contain confidential or sensitive information must have a data custodian for each source; each department must identify all sources of confidential/sensitive information and assign a data custodian. The data custodian and the user share the responsibility of preventing unauthorized access to PSCC information systems. The data custodian will analyze user roles and determine the level of access required to perform a job function. The level of authorized access must be based on the principle of least privilege.

Managers will notify Information Services of internal personnel changes in job function, status, referral privileges, and/or affiliation. Human Resources will notify Information Services of all terminations and personnel transfers to different departments. The data custodian will work with Information Services to update information system access no more than five (5) business days after being notified of terminations and no more than thirty (30) days after other personnel status changes.

Access to an information system must be reviewed regularly. User authorization shall be reviewed and revised by the data custodian. At a minimum, the data custodian must review user access to the information system every twelve (12) months and address issues.

Reviewed/Recommended: President's Council, November 24, 2014  
Approved: L. Anthony Wise, Jr., President, November 24, 2014