Employee access to the college’s administrative information system is based upon security classification levels and job roles. Security classification levels will be reviewed annually to ensure operational requirements are being maintained.

**Procedure 1016.1**

**Module Security Manager**

A module security manager is considered the owner of a module’s processes and data and, as such, is the individual who can authorize a specific security classification level to a college position within his/her respective administrative information system module. The following list contains the college’s current modules and their respective security manager:

- Student - Director of Admissions
- Finance - Comptroller
- Accounts Receivable - Comptroller
- Purchasing - Director of Procurement
- Financial Aid - Director of Financial Aid
- Human Resources - VP for Human Resources
- Budget Position Control - VP for Administrative Affairs
- Payroll - VP for Administrative Affairs

**Procedure 1016.2**

**Account Activation**

Access, including the required security class level, will be created automatically when an employee is assigned to a position in the administrative information system. Exceptions to modify the security class level will need to be approved by the respective administrative information system module security manager.

**Procedure 1016.3**

**Account Deactivation**

Access will be cancelled automatically when the employee’s position assignment is ended in the administrative information system.
Procedure 1016.4
Backend Data Changes

Any backend update made to processes or data stored in the college’s administrative information system must be approved by both the module security manager and the Systems Analyst assigned to the module.

Documentation in support of the update, as well as before and after images, will be placed by the analyst in a dated folder on a shared drive that is also accessible by the Director of Administrative Computing.

Updates to processes or data must include updating the activity date field as well as including the Oracle username of the Systems Analyst making the change in the user field (where possible).

Process and data updates will be made under the Systems Analysts login credentials. No updates will be made using the schema owner login credentials.

Procedure 1016.5
Monitoring Systems Access Logs

Systems access logs will be monitored and reviewed for unusual or suspicious activity using diverse mechanisms. Scripts will be run on a regular schedule looking for data changes initiated by privileged user accounts.