COCHISE COLLEGE

Administrative Policy

Category: Technology
Policy Number: 6003
Title: Administrative Information System - Employee Access

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

Procedure 6003.1
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 - Controller
- Accounts Receivable - Controller
- Purchasing - Director of Procurement
- Financial Aid - Director of Financial Aid
- Human Resources - VP for Human Resources
- Budget Position Control - Controller
- Payroll - VP for Human Resources

Procedure 6003.2
Account Activation

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

Procedure 6003.3
Account Deactivation

Access shall be cancelled when the employee's position assignment is ended in the administrative information system.

Procedure 6003.4
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 shall 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 shall be made under the systems analysts login credentials (where possible).

Procedure 6003.5
Monitoring Systems Access Logs

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