Operational Management Policy D 110

Purpose: To define and document operational standards and procedures necessary to minimize the risk of information loss or misuse

- All information processing facilities must document operating procedures, management processes and have formal incident management procedures relating to information security matters. Roles and responsibilities of affected individuals who operate or use the information process facilities must be defined and documented.
- Computing hardware, software or system configurations provided by the campus must not be altered or added to in any way unless exempted by documented written policy, procedures, or specific written approval of campus management.
- Where the campus provides a server, application, or network service to another campus, operational and management responsibilities must be coordinated between them.

Separation of Development, Test, and Production Environments
- Separation of the development, test, and production environments is required, either logically, or physically. Processes must be documented and implemented to govern the transfer of software from the development environment to production. The following controls should be implemented:
  - A clear separation of the production, test, and development environments must be maintained.
  - Access to compilers, editors, and other system utilities must be removed from the production system when not required.
  - Logon screens must be sufficiently identified for production, testing, and development.
  - Controls must be in place to issue short-term access to development staff to correct problems with production systems, allowing only necessary access.

Segregation of Duties
- To reduce the risk of accidental or deliberate system misuse, separation of duties or areas of responsibility must be implemented where practical.
- Whenever separation of duties is difficult to achieve, other compensatory controls such as monitoring of activities, audit trails, and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.
- Processes must be documented and implemented to govern the transfer of software from the development environment to production.
INQUIRIES/REQUESTS:

Chair, Information Security Steering Committee

Division of Information Technology, Office of the CIO
Educational Communications Center, Room 231
631-632-9085