

POLICIES AND PROCEDURES MANUAL

TITLE	Information Resources Security
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	February 3, 2000

authorized in writing by appropriate management and in conformance with security policies, procedures, and standards. Employees whose principal duties involve the modification of network architecture are considered appropriate managers.

7. No software program or information can be added to, or removed from, any operating system, database or file unless explicitly authorized in writing by appropriate management and in conformance with institutional security policies, procedures, and standards. Additionally, software that bypasses, in any manner, approved security software or controls may not be written or installed. In cases where a personal computer is assigned to a specific employee, that individual will be considered the owner of the information contained in that system and is therefore the appropriate manager as defined in this section.
8. Personnel shall not disclose any confidential or sensitive information unless it is properly required in their jobs, or except as authorized in writing pursuant to security policies. Such information includes technical and business information, information systems and software development and products and software licenses disclosed on a confidential basis to the institution.
9. On termination of employment or a contractual relationship with the Institution, or as otherwise requested by appropriate management, personnel must surrender all property and information managed by the Institution, and must not subsequently disclose any confidential or sensitive information.

Violation of this Policy:

Any person violating this policy is subject to immediate disciplinary action, which may include termination of employment, expulsion, or termination of a contract. In addition, there may be bases in which a person may be subjected to civil or criminal liability.