Personnel Security Policy D 109

All information, regardless of the form or format, which is created, acquired or used in support of the University’s activities, must be used only for its intended purpose. Information must be protected from its creation through its disposal. Information collected must be classified and protected based on its importance to the business activities, risks, and security best practices.

Each authorized user of University information has an obligation to preserve and protect it in a consistent and reliable manner. Security controls provide the necessary physical, logical, and procedural safeguards to accomplish this goal.

Individual Accountability

- Access to information must be limited to insure information integrity and accountability. Unique user IDs must be used with other more advanced technologies in cases where the information is highly confidential and applications/systems permit.
- An individual must access only the information that they are authorized to use and view.
- Each individual is responsible to protect against unauthorized activities associated with their userID.
- Individual user IDs and passwords must not be shared

Management of Personnel

- The information owner or their delegate must secure information within their jurisdiction based on the information’s value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.
- Information owners are responsible for determining who should have access to protected resources, within their jurisdiction, and what those access privileges will be (read, update, etc). These access privileges will be granted in accordance with the user’s job responsibilities.
- A user management process shall be established and documented by the campus to outline and identify all functions of user management, including the generation, distribution, modification, and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to the campus applications and information and that these users only have access to the resources required to perform their job functions.
- The user management process must include:
  - Enrolling a new user
  - Removing userids
  - Granting privileged accounts to a user
  - Removing privileged accounts of users
  - Periodic review of privileged accounts of users
  - Periodic review of users enrolled to any system
Assigning a new authentication token (PW Resetting process).
The appropriate information owner or authorized delegate will make requests for the registration and granting of access rights for campus employees.
Standards for the registration and management of user accounts for individuals that are not employed by the campus must include the credentials for those individuals and appropriate compliance agreements necessary to ensure that this access to information is limited in scope and that the individual understands and agrees to keep this information confidential and use it only for the purposes associated with their contract or agreement with the University.

INQUIRIES/REQUESTS:
Chair, Information Security Steering Committee
Division of Information Technology, Office of CIO
Educational Communications Center, Room 231
631-632-9085