Administrative Policy

Suffolk County Community College

Enterprise Systems Information Security Procedures

The following procedures apply to all College systems storing private or sensitive information. The purpose of the procedures is to outline and identify all functions of user management, to include the following:

- requests by the appropriate information owner or other authorized officer for the registration and granting of access rights for employees;
- enrolling new users;
- removing user-IDs;
- granting "privileged accounts" to a user;
- removing "privileged accounts" from a user;
- periodic review of "privileged accounts" of users;
- periodic review of users enrolled to any system; and
- assigning a new authentication token (e.g. password reset processing).

These practices are governed by the College's Information Security Committee (ISec).

A. **User Management**

1. **Protected Data Resources:** The following govern individuals' access to College information systems, including Banner, Oracle's Operational Data Store and Enterprise Data Warehouse, Department Websites and Network Folders.

    a. Role-based permissions will be the standard practice for providing user access to enterprise data resources.
    b. Users will be assigned roles based upon the functional requirements of their position at the College and only provided roles with as much access as necessary to handle these requirements.
    c. Additional levels of security will be setup when available to govern departmental-based access within a role (*e.g.,* access to specific accounts or organizations information within Financial or HR screens in Banner).
    d. Request for access must be approved by the systems' data owner.
    e. Users will maintain their access while they continue in the same department, in the same functional capacity.
    f. A user's access will be evaluated annually by the departmental supervisor.
    g. Permissions to data resources will be removed when an individual leaves their current assignment. New permissions will be established based upon the request of the new department and approval of the data owner.
        i. Department administrators are responsible for system use of individual assigned access within their administrative area, and must initiate both the request for individual access and the notification of termination using the appropriate forms.
        ii. Permission will take time to be evaluated so administrators need to initiate requests in advance of an individual's arrival.
        iii. Notification of termination should be received a week prior to a transfer or termination, and dated to take effect upon completion of the individual's last use of the system in the department or office.
        iv. In the event of an actual or suspected security violation, the department administrator must immediately notify the Office of Computer and Information Systems, providing information on the violation and risk level. The administrator must also follow-up with a report to the College Information Security Committee (ISec).

h. In addition to internal system documentation, a list of all system permissions for a user will be maintained in hardcopy and stored in a standard secure location by the Computer Center, such that permissions can be quickly identified and modified.

2. **Community Based Systems:** The following procedures govern individuals' access to College community-based systems including Email and ***MySCCC***.

   a. Individuals will be provided access to these systems based upon their membership in major groups at the College. The groups include but are not limited to: Employees, Employee Bargaining Unit, Student, Student Matriculation Status and Program, Alumni, and Retirees.
   b. Access to an individual's systems is based upon the policies established for these systems.
   c. Roles for the ***MySCCC*** portal will normally be maintained from records created in Banner.

B. Data Owners – Protected Data Resources

1. Each data resource will have an identified Data Owner with the responsibility and authority to determine who, based on job responsibilities, should have access to protected resources within their jurisdiction and what those access privileges are, such as "read," "update," etc.
   a. Data owners for College Protected Information are listed within the College's Information Security Policy.
   b. Department and Office Administrators are the data owners of department information resources including department websites and network shared folders.
   c. Committee chairs are the owners of committee resources including websites and Group shares within ***MySCCC***.

2. Data Owners for systems that contain protected information are responsible for developing roles, which encompass a set of permissions based upon functions. This is to be done in collaboration with Computer and Information Systems personnel. Access is to be approved based upon these roles.

3. Notwithstanding anything herein to the contrary the President of the College or his/her designee and the General Counsel of the College or his/her designee can grant access to any and all College data.

Note: While departments and office administrators own the material contained within their websites, Community Relations determines what is suitable for external publication.

Approved by Executive Council
March 21, 2011