**Administrative Policy**

## Suffolk County Community College

## Policy on Information Security Access

This policy covers the use, retention, and disposal of protected private or sensitive information (*Protected Information)* by individuals and departments given access to such information. This *Protected Information*, whether in reports, on forms or available through information systems, belongs to the College, is under the jurisdiction of the offices that follow and is available to others under specific guidelines.

**Oversight:** The Information Security (ISec) Committee is responsible for oversight of this policy. The following College officials are responsible for management of information for their respective areas of operations:

1. **Alumni**: Vice President for Institutional Advancement
2. **Continuing Education and Workforce Development**: Associate Vice President for Workforce and Economic Development
3. **Employees - Prospective Employees and Past Employees**: Assistant Vice President for Employee Resources
4. **Faculty and Visiting Scholars**: Vice President for Academic and Student Affairs
5. **Finance**: Vice President for Business and Financial Affairs
6. **Institutional Effectiveness** (including summary reports and research findings): Vice President for Planning and Institutional Effectiveness
7. **Legal** (including all Freedom of Information Requests): Deputy General Counsel
8. **Students**: Associate Vice President for Student Affairs
9. **Information within Electronic Systems** (responsible for the management of authorized access and safeguarding against unauthorized access):
    a. **College Administrative Systems**: Associate Dean for Computer and Information Systems
    b. **College Academic Systems** (as assigned): Associate Dean for Instructional Technology
    c. **Campus Systems**: Campus Technology Administrators

**Responsibilities:** All College faculty, staff and administrators have custodial responsibility for the information they are provided and must safeguard this information from unauthorized access and release. Administrators are further responsible for the maintenance and periodic update of information security procedures within their office or department and must periodically communicate these with their faculty, staff and administrators.

Third parties provided access to College information must abide by all College policies on information access and security. In addition, if not included in a contract, they must sign the College's non-disclosure agreement.

**Security Breaches and Cyber Security Incidents:** Any compromise to College protected information must be reported immediately to the College Deputy General Counsel, Executive Director for Safety and Security Compliance and the Associate Dean for Computer and Information Systems. These will be addressed in accordance with the ***NYS Information Security Breach and Notification Act*** (http://www.cscic.state.ny.us/security/securitybreach). Third parties assume liability for breaches that occur on information to which they have access and must also abide by the ***NYS Information Security Breach and Notification Act***.

Any unusual or serious cyber security incidents will also be reported as outlined by SUNY under the ***NYS Cyber Security Policy P03-001***. The College will follow New York State incident response procedure (http://www.cscic.state.ny.us/lib/policies/)

**Administrative Policy**

**Department-Based Procedures:** Each department and office with access to College information must have security procedures in place which meet the standards identified by the Information Security (ISec) Committee. These procedures must include the following:

- An identification of the data to which the office has access;
- An identification of how the data elements are used;
- A list of individuals who have access to the information; and
- A list of procedures for the management of paper copies of reports, screen prints, forms, and office files. At a minimum, these must include storage in locked desks or file cabinets of all documents containing personal or private information and shredding/ secure disposal of these documents when no longer needed. See College Procedures on ***Disposal of Documents Containing Personally Identifiable Information***.

**Department Data and Applications:** Departments are not normally authorized to collect private and sensitive information or develop data applications that store protected information. Data should be stored and applications built within College enterprise systems. Exceptions will only be considered when required functionality is not available within the enterprise environment. In this case, requests need to be justified to and approved by the data owners listed above.

**Department Shared Folder:** Department shared folders would not normally be used to store files containing personal or private information. Requests to use a shared folder to store protected information need to be justified to and approved by the data owners listed above. See the College ***Policy on Shared Departmental Network Folders***. Exceptions are network folders setup by IT to distribute reports and data extracts to limited controlled populations.

**Approved by Executive Council**
**March 21, 2011**