Administrative Policy

Suffolk County Community College

Management Standard of Protected College Information in Transit and Storage

This standard covers the movement and storage of protected private or sensitive information (*Protected Information*) outside of College systems, including its transit to and storage on network folders, desktops, laptops and portal media and transit to non-college systems. Access to this information by individuals and departments is governed by the College's ***Policy on Information Security Access*** and the ***Policy on the Protection of Social Security Numbers***. The Information Security (ISec) Committee is responsible for the oversight of this standard.

College Enterprise Systems

College *Protected Information* is stored by standard practice in secure College enterprise systems, under the jurisdiction of the Office of Computer and Information Systems. Data is only copied or removed from these systems to fulfill identified required needs. These needs are governed by the College's ***Policy on Information Security Access***.

Departments are not authorized to collect *Protected Information* or develop data applications that store *Protected Information* unless specifically authorized by College data owners according to the College's ***Policy on Information Security Access***.

Transit and Storage Standard

The following standards govern the protection of *Protected Information,* whether in transit or in storage outside College's enterprise systems:

1. *Protected Information* within the College's enterprise systems is only to be accessed from College authorized administrative devices (computers, laptops, etc.).

2. *Protected Information* in transit over the Internet, State or County Intranet, the College wireless or academic network, or a personal network connection (Bluetooth, infrared) is to be protected using the College's minimum encryption standard.

3. *Protected Information* will normally be transmitted to external systems using Secure File Transfer Protocol (SFTP) applications and methods. If SFTP is not available, files may only be transmitted using email or standard File Transfer Protocols (FTP) if the file is encrypted and password protected. However, anonymous FTP will never be used for transmission of *Protected Information*. In addition, only College email accounts are to be used to send and receive these files. Transmission methods must be approved by the College Associate Dean for Computer and Information Systems. Transmissions must also be logged, identifying the transmitter, transmission data and receiving location. Transmission logs are to be kept for one (1) year.

4. College reports and data extracts of *Protected Information,* for distribution to internal population, will normally be posted in network folders limited to approved users. If a secure network folder is not available, college email addresses may be used if the files are encrypted and password protected.

5. Files containing *Protected Information* are not to be stored on any shared folder or network resource, unless the folder is approved for this purpose as outlined under the College's information security procedures. These files cannot be stored on any network device that does not meet the College's ***Policy and Procedures on Access Control and Password Security***.

6. Files containing *Protected Information* approved for removal to an administrative desktop computer are to be stored in the individual's ***My Documents*** folder. This folder is a protected network resource.

7. College administrative laptops, because of their access to *Protected Information* within the College's enterprise systems, are to utilize full disk encryption that meets the College's encryption standard. Also see the College's ***Administrative Laptop Policy***.

8. Any third party laptop that has access or contains *Protected Information* must employ full disk encryption that meets the College standards.

9. *Protected Information* stored on devices outside of the systems noted above are to be protected by encryption at one of the following levels: full disk, volume level, folder level, file level or field level. Examples of devices include the following:

    a. Personal Digital Assistants *(PDAs);*
    b. USB Flash Drives; and
    c. Laptops with operating systems that do not support full disk encryption.

10. *Protected Information* stored on any removable electronic storage media must be encrypted according to the College's minimum encryption standard.

    Note: Due to the immaturity of tape encryption technology, an exemption may be made for tapes. The exemption must be processed and approved in writing by College's Executive Director of Risk Mitigation after receipt of a recommendation from the College ISec Committee. The exemption must include other mitigating controls. A record of the approved exemption shall be maintained by the College ISec Committee. The exemption will include a timeframe identifying when it will be reviewed by the College ISec Committee to certify that the need is still valid and required, and the controls in place are appropriate and current.

Approved by Executive Council
March 21, 2011