CCS Administrative Procedure
7.30.10-A

Implementing Board Policy 7.30.10
Contact: Director of Information Systems, 533-8018

1.0 Purpose

The purpose of this procedure is to outline the scope, requirements and responsibilities for developing, implementing, and maintaining the Information Technology (IT) standards detailed in the CCS Information Technology Security program. These standards apply to all CCS organizational units that operate or manage IT services and equipment in support of administrative and instructional services.

2.0 Scope and Requirements

2.1 IT Security is defined as protecting the integrity, availability, and confidentiality of information assets managed by CCS; specifically, protecting information assets from unauthorized release or modification and from accidental or intentional damage or destruction. Included is the protection of technology assets such as hardware, software, telecommunications, and networks (infrastructure) from unauthorized use.

2.2 The Washington State Department of Information Systems (DIS) establishes security standards that define the practices and procedures necessary for implementing an agency-specific IT security program. These standards apply to all IT activities, whether they are operated by or for an agency. They include specific steps that shall be taken to ensure a secure IT environment is maintained and all agency systems provide for privacy and security of confidential information. These standards include, but are not limited to:

- 2.2.1 Personnel Security
- 2.2.2 Physical Security
- 2.2.3 Data Security
- 2.2.4 Network Security
- 2.2.5 Access Security
- 2.2.6 Application Security
- 2.2.7 Operations Management
- 2.2.8 Electronic Commerce
- 2.2.9 Security Monitoring and Logging
- 2.2.10 Incident Response
- 2.2.11 Maintenance

2.3 The CCS IT Security Program applies to all faculty, staff, and administrators within the CCS community with specific duties and responsibilities placed upon the Information Technology (IT) departments at each of the four organizational units (District Administration, SCC, SFCC, and the IEL). It is the responsibility of all members of the college community to adhere to Board of Trustees Policy #7.30.10 Information Technology and the security standards directly affecting end users as identified in the IT Security Program.

3.0 Responsibilities

3.1 CCS management has the following responsibilities regarding the IT Security Program in accordance with the Washington State Information Services Board (ISB) Information Technology Security Policy:

3.1.1 Pursuant to RCW 43.105.017(3), agency heads are responsible for the oversight of their respective agency's IT security and shall confirm in writing that the agency is in compliance with these standards. The annual security verification letter shall be included in the agency IT portfolio and submitted to the ISB. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval. The head of each agency shall provide annual certification to the ISB by December 31 of each year that an IT Security Program has been developed and implemented. CCS submits one letter of compliance, signed by the chancellor, on behalf of all organizational units.

3.1.2 CCS shall have an audit performed once every three years for compliance with IT Security Policy and Standards. This audit shall be performed by parties independent of the agency's IT organization. CCS is required to maintain documentation showing the results of the audit and corrective action plans for any material deficiencies identified by the audit.

3.1.3 All IT security program documentation shall be written in a clear, compelling, non-technical manner. Some IT security program documentation may contain sensitive information about the agency's business, communications, and computing operations or employees. Such information is to be shared only with personnel who need it to perform their official duties. Security program documentation, as prescribed in RCW 42.17.310(1)(ww) and (ddd), should be clearly labeled as “Computer Security Information.”

3.2 Compliance with DIS Security Policies: CCS shall operate in a manner consistent with the goals of the DIS IT Security Policies and Standards to maintain a shared, trusted environment within the Washington Community and Technical College (WCTC) system for the protection of sensitive data and business transactions. CCS shall provide secure business applications, infrastructures, and procedures for addressing the business needs of its four operating units.

3.3 Principles of Shared Security: CCS subscribes to the following principles of shared security:

3.3.1 CCS shall assure that appropriate security standards are considered and met when developing or purchasing application systems or data access tools;

3.3.2 CCS shall recognize and support the necessity of authenticating external parties needing access to sensitive information and applications;

3.3.3 CCS shall develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network; and

3.3.4 CCS shall follow security standards established for creating secure sessions for application access.

3.4 Secure Internet Applications: CCS ensures that all Internet-based applications that conduct transactions for state business, with other public entities, citizens and business adhere to the DIS standards for developing and documenting secure Internet applications.

3.5 Employee Training: CCS ensures staff is trained in IT security awareness, and that technical staff receive the appropriate training commensurate with their job responsibilities.

3.6 Annual Review: CCS reviews its IT security processes, procedures, and practices annually and makes appropriate updates after any significant change to its business, computing, or telecommunications environment.

4.0 Related Information

4.1 Administrative Procedure 7.30.05-A – Acceptable Use of Information Technology Resources

4.2 RCW 43.105.017 – Legislative Intent

4.3 Contact information for CCS IT Support Departments

- District Office Help Desk: 533-8013
- SCC Help Desk: 533-8899
- SFCC Help Desk: 533-4357
- IEL Help Desk: 279-6010

Originated: November 2009
Cabinet approval: December 14, 2009