



ADMINISTRATIVE PROCEDURES

INFORMATION TECHNOLOGY SECURITY PROCEDURE

DECEMBER 16, 2003

Information Systems

**BOT POLICY
1.70.08**

**ADMINISTRATIVE PROCEDURE
1.70.08-A**

PAGE 1 OF 2

ADMINISTRATIVE PROCEDURE IMPLEMENTING BOARD POLICY 1.70.08 – IT SECURITY POLICY

PURPOSE

The purpose of this administrative procedure is to create an environment within the Community Colleges of Spokane (CCS) that maintains Information Technology (IT) system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data.

This procedure governs all other CCS standards and procedures pertaining to IT usage for on-campus and off-campus use and complies with the Washington State Department of Information Services (DIS) IT Security policies, standards and guidelines.

SCOPE

The scope of this procedure extends to all campus Information Technology facilities, equipment and services that are managed by Spokane Community College, Spokane Falls Community College, the Institute for Extended Learning and the district office as well as off-site data storage, computing and telecommunications equipment. This procedure also includes application-related services purchased from other state agencies or commercial concerns, and Internet-related applications and connectivity.

It is not the intent of the IT Security Policy and this procedure to restrict academic freedom in any way, therefore this procedure exercises the exemption granted in the Washington State Department of Information Services (DIS) Information Technology (IT) Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200 which states; "In the case of institutions of higher education, the provisions of chapter 20, Laws of 1992, apply to business and administrative applications but do not apply to academic and research applications."

IT security is defined as:

- Protecting the integrity, availability and confidentiality of information assets managed by CCS.
- Protecting information assets from unauthorized release or modification, and from accidental or intentional damage or destruction.
- Protecting technology assets such as hardware, software, telecommunications, networks (infrastructure) from unauthorized use.

The administrative procedure for this policy is:

1. **Compliance with DIS Security Policies:** CCS shall operate in a manner consistent with the goals of the Department of Information Systems 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.
2. **Principles of Shared Security:** Furthermore, CCS will subscribe to the following principles of shared security:



ADMINISTRATIVE PROCEDURES

INFORMATION TECHNOLOGY SECURITY PROCEDURE

DECEMBER 16, 2003

Information Systems

**BOT POLICY
1.70.08**

**ADMINISTRATIVE PROCEDURE
1.70.08-A**

PAGE 2 OF 2

- CCS shall assure that appropriate security standards are considered and met when developing or purchasing application systems or data access tools;
 - CCS shall recognize and support the necessity of authenticating external parties needing access to sensitive information and applications;
 - CCS shall develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network; and
 - CCS shall follow security standards established for creating secure sessions for application access.
3. **Secure Internet Applications:** CCS will ensure 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.
 4. **Employee Training:** CCS will ensure all staff is trained in IT security awareness, and that technical staff receive the appropriate training commensurate with their job responsibilities. .
 5. **Annual Review:** CCS will review its IT security processes, procedures, and practices annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment.
 6. **Compliance Audit:** CCS will conduct a compliance audit of its IT Security Policy and Standards once every three years in accordance to State Auditor's requirements. CCS will maintain documentation showing the results of its audit and the plan for correcting material deficiencies revealed by the review. The State Auditor may audit CCS IT security processes, procedures, and practices, pursuant to RCW 43.88.160 for compliance with this policy.
 7. **Oversight:** Pursuant to RCW 43.105.017(3), the executive for each of the four operating units of the Community Colleges of Spokane is responsible for the oversight of their respective IT security program and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter will be submitted to the ISB, as required. The verification indicates review and acceptance of CCS security processes, procedures, and practices as well as updates to them since the last approval. It is the responsibility of all members of the college community to adhere to this policy and the standards contained in the IT Security Program.

The CCS IT security standards and practices contain information that may be confidential or private regarding CCS business, communications, computing operations and employees. Persons responsible for distribution of these documents should consider the sensitive nature of the information as well as the related statutory exemptions from public disclosure See RCW chapter 42.17.

The board policy (1.70.08) associated with this procedure can be located at the CCS Intranet site: <http://ccsi.spokane.edu/manform.htm>