POLICY 4124

SECURITY POLICY FOR INFORMATION TECHNOLOGY RESOURCES

POLICY

Consistent with its mission and goals, Shoreline Community College will provide secure information technology resources to support the instructional and administrative activities of the institution. Security includes the ability to protect the availability, utility, integrity, authenticity, confidentiality and possession of information assets managed by the College. This policy is in accord with state and federal laws, established college rules, and negotiated agreements. It exercises the exemption granted in the Department of Information Services (DIS) Information Technology Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200. (RCW 43.105.200 provides an exemption from the DIS Information Technology Security Policy specifically for academic functions. It allows flexibility to develop a security policy that is appropriate for the educational environment, provided that it is consistent with the intent of the Information Services Board. The exemption does not apply to business and administrative functions.)

Approved by:
Board of Trustees 10/22/03
Recommended by:
College Council 10/14/03

Done in Open Meeting by the Board this 22nd day of October, 2003.

Board of Trustees

Shoreline Community College

By: /s/ Edith Loyer Nelson
Chair of the Board

SECURITY POLICY FOR
INFORMATION TECHNOLOGY RESOURCES

PROCEDURAL GUIDELINES

1. SCC will secure business applications, infrastructures, and procedures used for college business consistent with the Center for Information Services and IT Security Policies of DIS.

2. SCC will assure appropriate security standards are met when developing or purchasing applications systems or data access tools.

3. SCC shall recognize and support the necessity of authenticating external parties needing access to sensitive information and applications.

4. SCC will develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network.

5. SCC shall follow security standards established for creating secure sessions for application access.

6. A Technical Architecture Document (TAD) must be included with applications developed or purchased by SCC after June 2003. The TAD must include a description of the high-level structure, and details of the security considerations in design, implementation, and use of the application. The TAD will be reviewed early in the process and no later than pre-implementation. This procedure will apply to **ALL** internet-based applications. The TAD review will be documented for validation and audit purposes.

7. All staff will be trained in IT security awareness.

8. Technology Support Services staff will receive appropriate training commensurate with their job responsibilities as funding allows.

9. IT security policies and procedures will be reviewed annually and after any significant business practice or software changes.

10. SCC will conduct a compliance audit every three years. To assure policy compliance, the State Auditor may audit security processes, procedures and practices, pursuant to RCW 43.88.160. The State Auditor will determine the timeline and scope for their office or another third party to perform an independent audit. SCC will maintain copies of the audits and plans for

correcting material deficiencies revealed by the review or audit (RCW 42.17.310 and 42.17.330).

11. Security audit and review documentation will be maintained in Technology Support Services and a copy of non-confidential material will be available in the Library.

12. Pursuant to RCW 43.105.017(3), the Vice President for Administrative Services is responsible for the oversight of this policy and will confirm, in writing, that the agency is in compliance. An annual security verification letter will be submitted to the Information Services Board. The verification indicates the review and acceptance since the last approval.

Approved by:
President's Executive Staff 9/8/03
College Council 10/14/03