Shoreline
COMMUNITY COLLEGE

PROCEDURE

Policy Name:	Information Technology Security
Policy Number:	4124
Applicable Code/Law:	RCW 43.105

Procedural Guidelines

Shoreline Community College will provide secure information technology resources consistent with its mission and goals in support of College instructional and administrative activities. These required guidelines are applicable to all faculty, staff, students, visitors, patrons, vendors, contractors, tenants, renters, and any external third parties that support Shoreline Community College's educational, administrative, operational, or strategic mission.

The policy and procedural guideline establish and maintain appropriate levels of security and integrity for data exchange and business transactions; ensure effective authentication processes, security architecture(s), and trust fabric(s); provide timely and appropriate information technology (IT) security staff training; and maintain compliance, testing, and audit provisions.

1. Documentation

Shoreline Community College will develop, maintain, and follow information security guidelines and procedures as appropriate to the College and consistent with the intent of information security standards and best practices in accordance with WaTech Policy 141.10. Applicable security guidelines and procedures will be reviewed by November of each year as well as prior to and after any significant change to applications, processes, procedures, or infrastructure is proposed or implemented.

2. IT Risk and Security Assessment

The College will conduct an IT Risk and Security Assessment when introducing new systems or when changes are made to an existing computing environment. Appropriate security controls commensurate with the risk and complexity of the system will be implemented upon assessment completion. Risk Assessments on systems processing Category 3 data or higher (i.e. items specifically protected from disclosure by law) will be conducted every three years.

Security assessments will be conducted when new systems are added or existing systems are modified to ensure assessment of the effectiveness of security controls. Assessments will include testing of security controls to make sure unauthorized access attempts can be identified or stopped.

Procedures Adopted: 10/14/03
Procedures Revised by ET: 2/19/19

3. Education and Awareness

The College will document the knowledge, skills, and abilities required for personnel performing work affecting IT Security and ensure that personnel assigned IT Security responsibilities are competent to perform the required tasks.

New employees will receive training within the first 30 days of employment on security awareness that identifies the risks of data compromise, their role in prevention, and how to respond in the event of an incident as relevant to the individual's job function. Thereafter, all employees will receive security awareness training on an annual basis.

4. Auditing and Compliance

Shoreline will require that contractors comply with Office of the Chief Information Officer (OCIO) and College IT security standards relative to the services provided. An independent audit will be performed every three years to assess compliance with OCIO IT security standards. The College will ensure the audit is performed by qualified parties independent of Shoreline Community College and submit the results of the audit to the state Chief Information Security Officer.

Procedures Adopted: 10/14/03
Procedures Revised by ET: 2/19/19