INFORMATION SECURITY POLICY

Technology Services
Policy Number: 6040

1.0 PURPOSE

Columbia Basin College (CBC) is obligated to provide adequate security and protection for all Information Technology (IT) resources within its ownership and control. This policy serves as an umbrella that governs all other CBC policies pertaining to IT usage on campus and complies with the Office of the Chief Information Officer (OCIO) policies.

2.0 AUTHORITY & SCOPE

2.1 Authority: Chapter 42.56 RCW; **C**hapter 43.88.160 RCW; **C**hapter 43.105.200 RCW; Payment Card Industry – Data Security Standards (PCI-DSS): 12.1.1; 12.1.2; 12.1.3; 12.1.4; 12.6.1; 12.6.3; 12.6.3.2.

2.2 Scope: This policy applies to employees, students, guests, contractors, consultants, temporary employees, and all personnel affiliated with Columbia Basin College. Specific duties and responsibilities are placed upon employees within the Technology Services (TS) department. This policy applies to all campus facilities, equipment and services that are managed by Columbia Basin College's Technology Services department, including off-site data storage, computing, and telecommunications equipment. This policy also applies to application-related services purchased from other state agencies or commercial concerns, and internet-related applications and connectivity.

2.2.1 Intended Exemptions: It is not the intent of this policy to restrict academic freedom in any way, nor to impinge on the intellectual property rights of authorized users, therefore this policy exercises the exemption granted in the Washington State OCIO Securing Information Technology Assets Policy.

Columbia Basin College's intent is to take precautions to prevent revealing specific security policies, standards, and practices containing information that may be confidential or private regarding Columbia Basin College business, communications, and computing operations or employees. Persons responsible for distribution of these documents should consider the sensitive nature of the information as well as related statutory exemptions from public disclosure (See RCW 42.56).

3.0 DEFINITIONS

3.1 Availability means data is accessible when you need it.

3.2 Commercial Concern is any entity or organization that provides goods or services on a for profit basis.

3.3 Confidentiality refers to protecting information from unauthorized access.

3.4 Information Assets are defined as all types of data stored or transmitted on behalf of the college. This may include (but is not limited to) employee data, student data, or college operations data.

3.5 Information Technology (IT) is a term that broadly defines all types of technology-delivered resources such as information, data, databases, equipment, applications, software, or web-based resources.

3.6 Integrity means data is trustworthy, complete, and has not been altered or modified by an unauthorized user.

3.7 Office of the Chief Information Officer (OCIO) is The Washington State Office of the Chief Information Officer (OCIO)

3.8 Office of the Chief Information Officer - Securing Information Technology Assets Policy is the published policy of the Washington State Office of the Chief Information Officer regarding information technology security. The purpose of this policy is to create an environment within State of Washington agencies that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data.

3.9 Policy is the official or prescribed plan or course of action used to guide and determine present and future decisions.

3.10 Security Standard is something established by authority, custom, or general consent as a model; OR something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality.

3.11 Technology Assets are defined as all software, hardware, or network infrastructure owned by the college.

3.12 Unauthorized Use pertains to any action that is in conflict or directly violates Columbia Basin College policies or standards for campus technology usage. This also includes unlawful use in violation of local, state and/or federal law.

4.0 POLICY – IT SECURITY

It is the sole responsibility of Technology Services to provide oversight management of all tasks and procedures that directly pertain to maintaining IT security on campus. It is the obligation of all members of the college community to support IT security by following all policies and procedures pertaining to technology resources and usage on campus.

4.1 IT security encompasses:

4.1.1 Protecting the integrity, availability and confidentiality of information assets managed by Columbia Basin College.

4.1.2 Protecting information assets from unauthorized release or modification, and from accidental or intentional damage or destruction.

4.1.3 Protecting technology assets such as hardware, software, telecommunications, and networks (infrastructure) from unauthorized use.

4.2 IT security will be maintained by upholding the following policies, standards, and guidelines:

4.2.1 Columbia Basin College will operate in a manner consistent with the goals of the OCIO Securing Information Technology Assets Policy to maintain a shared, trusted environment within Columbia Basin College and within the Washington Community and Technical College (WACTC) system for the protection of sensitive data and business transactions.

4.2.2 Columbia Basin College will maintain an IT security audit portfolio that includes comprehensive documentation of all processes, including IT applications developed or purchased, as required by the OCIO Securing Information Technology Assets Policy.

4.2.3 Columbia Basin College will ensure that all college employees are appropriately familiar with relevant IT security policies and procedures and are aware of their personal responsibilities to protect IT resources on campus. Columbia Basin College will provide training to each employee in the cyber or data security procedures for which they are responsible.

4.2.4 Columbia Basin College will review its security processes, policies, procedures, and practices annually. In the event of any significant changes to its business, computing, or telecommunications environments, Columbia Basin College will make appropriate updates as necessary.

4.2.5 A compliance audit of this Information Security policy will be conducted every three years and will be performed by knowledgeable parties independent of Columbia Basin College employees, such as the state auditor (OCIO-141). The format of this work shall follow audit standards developed and published by the Washington State Auditor. The state auditor's office may determine if an earlier audit of some or all of Columbia Basin College IT processing is warranted, in which case they will proceed under their existing authority. Columbia Basin College will maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulae, designs, drawings, computer source codes, objects codes or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure. (See RCW 42.56). The state auditor may audit Columbia Basin College IT security processes, policies, procedures, and practices, pursuant to RCW 43.88.160 for compliance with this and the OCIO Securing Information Technology Assets Policy.

4.3 Responsibilities

4.3.1 Department Leaders and Supervisors are responsible for:

4.3.1.1 Ensuring that all employees are appropriately familiar with relevant IT security policies and procedures and are aware of their personal responsibilities to protect IT resources on campus.

4.3.2 Employees are responsible for:

4.3.2.1 Taking all required training; to be appropriately familiar with relevant IT security policies and procedures; and are aware of their personal responsibilities to protect IT resources on campus.

4.3.2.2 Annually acknowledging they have read and understand the Information Security Policy and Security Awareness and Acceptable Use Policy.

4.3.3 Technology Services is responsible for:

4.3.3.1 Maintaining an IT security audit portfolio on behalf of the college that includes comprehensive documentation of all processes as required by the Washington state OCIO Securing Information Technology Assets Policy.

4.3.3.2 Providing the college with secure business applications, services, infrastructures, and procedures for addressing the business needs of the college.

4.3.3.3 Following and enforcing internal security standards established for creating and maintaining secure sessions for application access.

4.3.3.4 Notifying Human Resources and the individual's direct supervisor when an individual or individuals have knowingly compromised IT security on campus. The responsibility for determining disciplinary action for individuals who may deliberately violate IT security policies will be managed by Human Resources, individual's direct supervisor, or local law enforcement, depending on the scope and nature of the violation.

4.3.4 Chief Information Security Officer

Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of the Leadership Team.

5.0 FORMS & OTHER RESOURCES

The Washington State Office of the Chief Information Officer (OCIO)
Office of the Chief Information Officer (OCIO) policies
RCW 42.56
RCW 43.88.160
RCW 43.105.200
OCIO-141: Securing Information Technology Assets Policy
PCI-DSS V4.0.1: Requirements: 12.1.1; 12.1.2; 12.1.3; 12.1.4; 12.6.1; 12.6.3; 12.6.3.2

6010 – Security Awareness and Acceptable Use Policy
10010 – Data Governance Policy

6.0 HISTORY & POLICY CONTACT

6.1 Originated: 02/2025.
6.2 Revised: N/A.
6.3 Proposal Date: 05/06/2025.
6.4 Policy Review: N/A.
6.5 Promulgation Date: 06/2025.
6.6 Responsible Administrator: Director for Technology Services.