SECURITY AWARENESS & ACCEPTABLE USE POLICY

Technology Services
Policy Number: 6010

1.0 PURPOSE

The purpose of this policy is to outline security awareness and acceptable use of computer equipment and to protect employees, students, and Columbia Basin College (CBC). Inappropriate use exposes Columbia Basin College to risks including virus attacks, compromise of network systems, data, services, and legal issues.

Columbia Basin College is committed to protecting all employees, students, partners, and the college from illegal or damaging actions by individuals, either knowingly or unknowingly. The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust, and integrity.

Systems and resources, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Web browsing, and File Transfer Protocol (FTP), are the property of Columbia Basin College. These systems are to be used for business purposes in serving the interests of the college, our students, employees, and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Columbia Basin College employee, student, and partner who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 AUTHORITY & SCOPE

2.1 Authority: Chapter 42.56 RCW - Washington Public Records law; Chapter 42.52.160 RCW - Washington Ethics law; Chapter WAC 292-110-010 WAC - Use of State Resources; Family Education Rights and Privacy Act (FERPA); Payment Card Industry – Data Security Standards (PCI-DSS): 4.2.2; 5.2.1; 5.3.1; 5.3.2; 5.4.1; 8.2.8; 8.3.9; 10.2.1.3; 12.2.1; 12.6.3; 12.6.3.1; 12.6.3.2.

2.2 Scope: This policy applies to employees, students, guests, contractors, consultants, and all personnel affiliated with Columbia Basin College. This policy applies to all equipment that is owned, used, or leased by Columbia Basin College.

3.0 DEFINITIONS

3.1 Hosts – Primary computing systems; can be workstations, laptops, or servers.

3.2 PAN – Acronym for Primary Account Number in Payment Card Industry (PCI) documentation.

3.3 Screen Lock - a process that protects the screen and access to data by automatically producing a moving image, slide show, or blanking the screen if the computer has been idle for a pre-determined amount of time. It requires the entry of username and password to unlock.

3.4 Spam - Unwanted, unsolicited bulk messages, often for commercial purposes.

4.0 GENERAL USE AND OWNERSHIP

4.1 While Technology Services administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the college systems remains the property of Columbia Basin College. Due to network security requirements, the confidentiality of employee's personal information stored on any network device belonging to Columbia Basin College cannot be guaranteed.

4.2 With the exception of certain personal uses considered de minimis under RCW 42.52.160(3) and WAC 292-110-010, Columbia Basin College's information systems and services are provided exclusively for furtherance of CBC's educational objectives, research, administrative processes, and CBC sponsored community service activities, and shall be used only for purposes consistent with the mission and goals of Columbia Basin College. Personal use of email and the Internet are specifically included in the de minimis exemption only when such use complies with governing law and college policy.

4.3 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Web systems. In the absence of such policies, employees should be guided by this policy on personal use, and if there is any uncertainty, employees should consult their supervisor.

4.4 Per CBC's 10010 – Data Governance Policy, section 4.4.2, sensitive and confidential data (Categories 2, 3 and 4) must be encrypted. Users (or device) must encrypt Primary Account Numbers (PAN) and other cardholder data when transmitting this type of information.

4.5 For security and network maintenance purposes, authorized individuals within CBC's Technology Services department may monitor equipment, systems, and network traffic at any time. Such monitoring may be place, system, and time specific, and on a case-by-case basis.

4.6 Columbia Basin College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.0 SECURITY AND PROPRIETARY INFORMATION

5.1 Per subsection 4.1 – 4.1.2.2 and subsection 4.3.5 of 10010 – Data Governance Policy, the user interface for information contained on Web-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: credit card information, non-directory student information, college strategies, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

5.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed every ninety (90) days.

5.3 All laptops and desktops should be secured with a password-protected screen lock with the automatic activation feature set at fifteen (15) minutes or less.

5.4 Employees should secure their workstations by logging off or locking the system (control-alt-delete for Windows users) when the workstation will be unattended.

5.5 All remote-access technologies must be configured to automatically disconnect sessions after thirty (30) minutes of inactivity.

5.6 Use encryption of information in compliance with CBC 10010 - Data Governance Policy.

5.7 Because information contained on portable computers is especially vulnerable, special care should be exercised. Technology Services shall configure and protect CBC laptops in accordance with TS Department System Configuration Procedure, including personal firewalls.

5.8 Postings by employees from a Columbia Basin College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Columbia Basin College, unless posting is in the course of business duties.

5.9 All workstations used by the employee that are connected to the Columbia Basin College Web, whether owned by the employee or Columbia Basin College, shall be continually executing approved anti-malware or anti-virus software with current definitions.

5.10 CBC shall deploy processes and automated mechanisms to detect and protect personnel against phishing attacks.

5.11 Employees and students must use extreme caution when opening email attachments received from unknown senders, which may be harmful to campus IT systems.

5.12 All Employees must participate and shall receive security awareness training as follows:

- Upon hire and at least once every 12 months.
- Multiple methods of communication will be used (e.g. online training, T&LPD sessions, etc.).
- Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to:
    - Phishing and related attacks.
    - Social engineering.
    - Periodic Phishing Campaigns deployed to assist employees in maintaining awareness of trends in phishing attacks.
    - Other additional training as assigned by Technology Services (TS) that is based on the nature of specific roles.
- Employees acknowledge and attest at least once every 12 months that they have read and understood the Information Security Policy and the Security Awareness & Acceptable Use Policy.

6.0 UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee or student of Columbia Basin College authorized to engage in any activity that is illegal under local, national, or international law while utilizing Columbia Basin College owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

6.1 Systems and Network Activities

The following activities are strictly prohibited, with no exceptions:

- **6.1.1** Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Columbia Basin College.
- **6.1.2** Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Columbia Basin College or the end user does not have an active license is strictly prohibited. While limited use of copyrighted content may be permitted under the principles of Fair Use for educational purposes, such use must comply with applicable copyright law. Additionally, all use of licensed databases, streaming services, and other digital content must adhere to the terms and conditions of their respective contractual agreements.
- **6.1.3** Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Technology Services management should be consulted prior to export of any material that is in question.
- **6.1.4** Downloading or installing any application not authorized by Technology Services. This includes the installation or use of personally owned applications.
- **6.1.5** Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- **6.1.6** Revealing your account password to others or allowing use of your account information by others. This includes family and other household members.
- **6.1.7** Using a Columbia Basin College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws or policies.

6.1.8 Making fraudulent offers of products, items, or services originating from any Columbia Basin College account.

6.1.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

6.1.10 Committing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, for purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

6.1.11 Port scanning or security scanning is expressly prohibited unless prior requests to Technology Services are made and written authorization from the Director for Technology Services is received.

6.1.12 Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.

6.1.13 Circumventing user authentication or security of any host, network, or account.

6.1.14 Reading, deleting, copying, or modifying the files, electronic mail or other data belonging to users without proper authorization.

6.1.15 Tampering with any system or network logging mechanism.

6.1.16 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

6.1.17 Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, VPN connection, or secure web session via any means, locally or via the Web.

6.1.18 Providing non-directory information about, or lists of, Columbia Basin College employees to non-contracted parties.

6.1.19 Providing information about, or lists of, Columbia Basin College students without following FERPA requirements.

6.2 Email and Communications Activities

6.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

6.2.2 Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

6.2.3 Unauthorized use, or forging, of email header information.

6.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

6.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6.2.6 Sending spam emails (unwanted or unsolicited messages) to external entities, whether from CBC's network or through other Web services,

to promote or advertise something that's hosted by the college or connected to CBC's network.

6.2.7 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7.0 VIOLATION & ENFORCEMENT

7.1 Students

Violation of the policy and procedures while using CBC systems and network resources could result in loss of access to IT resources. Student violation is subject to disciplinary action under the Student Rights & Responsibilities.

7.2 Employees

Violation by employees is subject to the appropriate discipline process up to and including dismissal, and also consistent with the provisions of the appropriate collective bargaining agreement(s).

7.3 Contractors and Third-Party Entities

Violation by contractors and third-party entities is subject to the appropriate action which may include, but is not limited to, one or more of the following:

- Denial of access to CBC technology resources;
- Removal from CBC campus;
- Cancellation of user account(s);
- Cancellation of work agreements with Columbia Basin College.

8.0 FORMS & OTHER RESOURCES

PCI-DSS V4.0.1: Requirement(s): 4.2.2; 5.2.1; 5.3.1; 5.3.2; 5.4.1; 8.2.8; 8.3.9; 10.2.1.3; 12.2.1; 12.6.3; 12.6.3.1; 12.6.3.2
NIST 800.171
Washington Public Records law (Chapter 42.56 RCW)
Family Education Rights and Privacy Act (FERPA)
Washington Ethics law (Chapter 42.52.160 RCW)
Use of State Resources (WAC 292-110-010)
1080 - Code of Ethic's Policy
10010 - Data Governance Policy
1090 - Standards of Conduct Policy
1020 - Non-Discrimination & Harassment Policy

9.0 HISTORY & POLICY CONTACT

9.1 Originated: 07/2009.
9.2 Revised: 03/2025.
9.3 Proposal Date: 05/06/2025.
9.4 Policy Review 03/18/2025.
9.5 Promulgation Date: 06/2025.
9.6 Responsible Administrator: Director for Technology Services.