Philosophy Statement

Big Bend Community College (BBCC) has a strong commitment to intellectual growth and to extended access of educational opportunities. Because of these philosophical commitments, BBCC supports the use of technology as both an analytical tool and a means to expand access to both information resources and educational opportunities. In order to support these commitments, the following operational policies have been implemented. These policies apply to all users of BBCC technology facilities and equipment. These policies also supplement the Community and Technical College Network Acceptable Use Policy, which is in place for college employees. Failure to comply with these policies may result in disciplinary action as specified in this document.

(For full text of CIS policy, see http://www.ctc.edu/~ctcadmin/WCTC_Acceptable_Use_Policy.html)

AP 8053

IT Security

It is the sole responsibility of IT to provide oversight management of all tasks and procedures that directly pertain to maintaining IT security on campus. It is the responsibility of all members of the college community to participate and share this obligation, as specified by all supportive policies and procedures pertaining to technology use on campus.

IT security is defined as:

Protecting the integrity, availability and confidentiality of information assets managed by BBCC.

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.

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

BBCC will operate in a manner consistent with the goals of the DIS IT security policy to maintain a shared, trusted environment within BBCC and within the Washington Community and Technical College (WACTC) system for the protection of sensitive data and business transactions.

BBCC will maintain an IT security audit portfolio that includes comprehensive documentation of all processes, as required by the Washington State DIS IT security audit process. This portfolio and all documentation related to any BBCC IT security policies will be maintained in the office of the Big Bend Technology Department (BBT).

BBCC will submit annual written verification to the Washington State DIS verifying compliance with the processes and documentation of processes required by the DIS IT Security Audit Process.

BBCC will ensure that all college employees are appropriately familiar with all IT security policies and procedures, and are aware of their personal responsibilities to protect IT resources on campus. BBCC will provide training to each employee in the security procedures for which they are responsible.

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

A compliance audit of the BBCC IT Security Policy will be conducted every three years and will be performed by knowledgeable parties independent of BBCC employees, such as the state auditor. 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 BBCC IT processing is warranted, in which case they will proceed under their existing authority. The nature and scope of the audit must be commensurate with the extent that BBCC is dependent on secure IT to accomplish its critical business functions. BBCC 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 42.17.310 and 42.17.330.) The state auditor may audit BBCC IT security processes, policies, procedures, and practices, pursuant to RCW 43.88.160 for compliance with this and the DIS IT Security Policy.

RESPONSIBILITIES

Big Bend Technology (BBT)

Big Bend Technology is responsible for:

Maintaining an IT security audit portfolio on behalf of the college that includes comprehensive documentation of all processes as required by the Washington State DIS IT security audit process.

Submitting, on behalf of the college, annual written verification to the Washington State DIS showing the college's direct compliance with all IT security standards, as outlined in the DIS IT security policy (RCW 43.105.017(3). This written verification will include all revisions from previously submitted documentation, and will be submitted no later than November 26 each year, as required by state law.

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

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

Notifying human resources and the appropriate administrator(s) when an individual or individuals have knowingly compromised IT security on campus. Big Bend Technology is not responsible for determining disciplinary action for individuals who may deliberately violate IT security policies. This responsibility will be managed by the respective campus office, administrator, or local law enforcement, depending on the scope and nature of the violation.

DEFINITIONS

Department of Information Services (DIS)

The Washington State Department of Information Services (DIS).

Department of Information Services IT Security Policy

Also called the DISIT Security Policy or the DIS IT Security Policy. This is the published policy of The Washington State Department of Information Services 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.

Information Assets

'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 personal data or college data.

Technology Assets

'Technology assets' are defined as all software, hardware, or network infrastructure owned by the College.

Unauthorized use

Unauthorized use pertains to any action that is in conflict or directly violates BBCC policies or standards for campus technology usage. This also includes unlawful use in violation of local, State and/or Federal law.

Information Technology (IT)

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.

Policy

A policy is the official or prescribed plan or course of action. Webster's 7th New Collegiate Dictionary defines "policy" as a "course or method of action selected from among alternatives…to guide and determine present and future decisions."

Security Standard

Webster's defines "standard" as "Something established by authority, custom, or general consent as a model or example; OR something set up and established by authority as a rule for the measure of quantity, weight, extent, value or quality." In order to protect resources and enable security audits the Information Services Board (ISB) required all state agencies adhere to common IT security standards.

RELEVANT LAWS AND OTHER RESOURCES

RCW 42.17.310
RCW 42.17.330
RCW 43.88.160
RCW 43.105.200

8053.1 Access

BBCC computing and networking resources are state property. Use of BBCC's computing and networking resources is a privilege. The access provision applies to all users, including but not limited to, students, college faculty, staff, and community users of library services. Additionally, individual labs may limit access to students currently enrolled in specific courses and each computer lab may charge lab fees accordingly. Individual units within the college may define conditions of use for facilities under their control. These statements shall be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. In addition, any network traffic exiting the college is subject to the acceptable use policies of the network connectivity providers.

8053.2 Network Misuse/Actions that are <u>Prohibited</u> on the College Network

A. Illegal Activities

The college network and computing facilities shall not be used to transmit any communication in any form (e.g. text, images, sound) where the content and/or meaning of the message or its transmission or distribution would violate any applicable law or regulation. All BBCC resources shall be used in strict accordance with all local, state, and federal laws.

B. Sharing and Copying Passwords

All computer account passwords are confidential and shall not be shared with others. The sharing of passwords constitutes a threat to network security. Passwords on accounts shall be changed frequently and not shared with other users. Community users shall not be provided with passwords to any college networks. Unauthorized copying of passwords belonging to others or the college is unethical and may constitute theft.

C. Hacking and Interference in Operation

Using the college network to gain unauthorized access to **any** computer system is forbidden. Knowingly performing an act that will interfere with the normal operation of technology facilities and/or computer workstations is not allowed, i.e., disabling computers or network services, consuming disproportionate resources that deny others reasonable access, and/or inducing substantial costs to the college.

D. Network Traffic

Sending chain letters is prohibited. Knowingly running or installing on any computer system, or network, or giving another user a program intended to damage or to place excessive load on a computer system or network is forbidden.

E. Breach of Security

The following activities are not allowed (except by personnel under direction of network administration):

- Attempting to circumvent data protection schemes or uncover security loopholes; and
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without obtaining explicit written agreement of the owner.

F. Unauthorized Copying or Modification of Files

In addition to constituting a breach of security, the unauthorized copying or modification of files belonging to others or the college may constitute plagiarism or theft. Modifying files without authorization is unethical and may be illegal.

G. Identity of User/Abuse of Account(s)

Misrepresenting in any manner, your identity, your account, or a computer in any email communication is absolutely forbidden. Sending anonymous email is not allowed. Unauthorized use of another user's account is not allowed.

H. Violation of Copyright Restrictions, Intellectual Property Rights, Software License Agreements, and Unauthorized Software Installation

Users shall comply with copyright laws. Therefore, no duplication of software, images, music, video files, or other intellectual materials that are subject to copyright is permissible. Users shall comply with all local, state and federal laws and restrictions that apply to the use of any and all copyrighted materials. No copyrighted software may be placed on any hard disk system without prior written authorization from the copyright owner.

Copying the files of others may constitute a violation of intellectual property rights. Therefore, prior written permission shall be obtained from the owner before any intellectual information is duplicated in any form.

Users are required to comply with software licensing agreements. Much of the software provided through the college for use by faculty and staff is subject to software license agreements. Software shall be used in compliance with the applicable software license agreement. Installing unlicensed or unauthorized software on BBCC equipment is prohibited.

I. Unauthorized Movement of Equipment

Any movement of computer equipment within the college shall follow established inventory procedures. Students are not allowed to move equipment unless they are employed by the college and have received permission from the appropriate college administrator and/or supervisor to do so. College equipment shall not be removed from campus for use in another location unless written permission is obtained from the appropriate Dean or Vice President. In some cases, this permission will not be granted because of grant or gift restrictions.

J. Restricted Application Use

Restricted application use is the use of applications not clearly related to the core purpose of the college, or which violate general college policy, jeopardize its state accredited status, or otherwise interfere with applications vital to everyday operation.

These applications include, but are not limited to, those that are illegal, such as fraud, harassment, copyright violation, and child pornography. Also, applications that deprive other users of their fair share of information technology or interfere with the functioning of central networks and systems, such as mass mailings, chain letters, unauthorized high-bandwidth applications, or denial of service attacks are prohibited. Disclaimers do not render restricted application use acceptable.

8053.3 Consequences of Misuse

A. Disciplinary Provision

Individual disciplinary actions shall follow college grievance and disciplinary procedures and policies applicable to faculty, employees, and students. Efforts will be made to resolve problems at the lowest departmental or divisional level.

Misuse of computing, networking, instructional technologies and/or information resources by any individual may result in the loss of privileges. Failure to comply with this policy may result in termination of the account and contents and loss of computing access privileges. The college may also require reimbursement costs by any user, which, if not paid, may necessitate further disciplinary action. Additionally, misuse of any of the above mentioned resources (in particular, computer accounts) by any individual may require financial restitution to the college for funds expended and could result in civil action and/or criminal action. Additionally, students, faculty and staff may be subject to disciplinary action up to and including termination or dismissal.

B. Legal Defense

BBCC considers illegal use of the college's computers, networks, or software an unauthorized activity by students, faculty, staff, and community users. Additionally, it is considered outside the scope of work of faculty, staff, and volunteers. Therefore, a legal defense will not be authorized in a proceeding instituted against individuals who engage in illegal use of the college's computers, networks or software unless otherwise authorized by law.

8053.4 Other Miscellaneous Provisions

A. Resource Limitations

Limitations or restrictions may be applied by system administrators on computing resources, such as storage space, time limits, or amount of resources consumed. Such restrictions ensure fair access for all users.

B. Accounts/Data

Student accounts on college computing systems will be administered and reviewed by staff as required for system management and administration. Student accounts or authorized user files will exist on a system as long as a student is enrolled in the particular program or course. Students are responsible for backing up their own data at all times onto their own floppy disks. BBCC disclaims responsibility for loss of data, and individual account contents. (Also, see section 9053.2(B) above, Sharing and Copying Passwords.)

BBCC makes no warranty of any kind, expressed or implied, regarding computer resources or services, or the contents of resources or electronic messages over the BBCC college network or connected networks. BBCC will not be liable, in any event, for incidental or consequential damages, direct or indirect, resulting from the use of the BBCC network or network services.
Use of BBCC's computing and networking resources is a privilege that depends on appropriate use of these resources. BBCC reserves the right, without notice, to limit or restrict individual use and hours of operation; to inspect, copy, or remove data, file, or system resources; and to log and audit activities on computing systems.

C. Web Pages/Internet/Intranet—General and Web Pages

BBCC is a provider of online services. All Internet or intranet publishers (this includes world-wide web publishers), whether they are divisions, departments, college organizations or individuals, are responsible for the content of the pages they publish and are required to comply with all BBCC policies and procedures as well as state and federal laws. The use of internet, intranet, or web pages which violate BBCC policies and procedures, as well as state and federal

laws, is prohibited and may result in disciplinary actions as set forth in Section 8053.3 of this policy.

Student Web Pages

Students may put web sites on the college server in furtherance of their education or as a part of their educational objectives. Although a "real world" project has the potential for great educational benefit, college resources cannot be used for commercial gain. Therefore, any student site that has any relation whatsoever to non-college business pursuits **shall be directly related to a class assignment**. Any web site that falls within this category shall be deleted from the college server on or before the last day of finals for the quarter within which the assignment was given. The students shall not host any site falling within this category on any site external to the college, and the address shall not be given out to any external agency.

D. Right of Agency/System Administration

The College network is subject to a variety of laws including, but not limited to:

- Use of state property (i.e., computers) is limited by state employees to purposes related to official duties by RCW 42.52.160;
- Use of state property (i.e., computer facilities/equipment) is prohibited for political purposes by RCW 42.52.180;
- Criminal liability for computer trespass could result in a felony conviction pursuant to RCW 9A.52.110 *et seq;*
- Criminal charges could result if users alter, damage, obliterate or erase records, information, data or computer programs pursuant to RCW 9A.48.100; and
- Materials prepared on the college's computer system may be subject to release as a public record (i.e., email, letters, memos); even deleted information from a back up system may be retrieved in the course of litigation pursuant to the Washington State Public Records Law, RCW 42.17.020 *et seq*.

BBCC maintains the right to inspect and monitor the use of computers to ensure compliance with college policy and all applicable state and federal laws.

Additionally, to maintain the function and operation of technology facilities and to protect them against unauthorized use, BBCC reserves the right to take whatever steps it deems appropriate to remedy or prevent activities that in its judgment, endanger the orderly operation of its networks or systems and/or which threaten the college's network connections to the internet and/or other institutions or networks.

When any use of information technology using the college network presents an imminent threat to other users or the network infrastructure, system operators may take whatever steps necessary to isolate the threat, without notice, if circumstances so require. This may include changing passwords, locking files, disabling computers, or disconnecting specific devices or entire networks from college, regional, or national voice and data networks. System operators will restore connectivity and functionality as soon as possible after they identify and neutralize the threat.

A computer owned personally by a student, faculty member, or staff member is subject to college policy while it connects to the college network directly or through a dial up connection. An individual shall not grant access privileges to other individuals on a computer in violation of the general use policy, even if that computer is personally owned. If a computer is connected to the college network, access from that computer to the rest of the college network shall only be made available to individuals otherwise authorized to use the college network. This includes email, listservs, web services, file transfer, Internet Relay Chat (IRC), telnet, and any other network traffic.

I, the undersigned, acknowledge that I have read, fully understand, and agree to follow BBCC's Technology Use Policy and Procedures (AP8053).

_____

User Signature Date