BOARD POLICY

BP8053 INFORMATION TECHNOLOGY (IT) SECURITY POLICY BP8053

Big Bend Community College (BBCC) acknowledges the obligation to provide adequate security and protection of all Information Technology (IT) usage within its domain of ownership and control. This policy serves as an umbrella that governs all other BBCC policies pertaining to IT usage on campus and is intended to comply with the Washington State Office of the Chief Information Officer (OCIO) Standard No. 141.10: Securing Information Technology Assets.

(For full text of OCIO policy, see http://ofm.wa.gov/ocio/policies/documents/141.10.pdf)

The BBCC IT Security Policy is acknowledged as a "living" document that may require alteration periodically to address changes in technology, applications, procedures, legal and social imperatives, and unanticipated dangers.

Applicability
This policy applies to all members of the BBCC community, with specific duties and responsibilities placed upon departments within Big Bend Technology (BBT). This policy applies to all campus facilities, equipment and services that are managed by the Big Bend Technology 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.

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 Office of the Chief Information Officer (OCIO) Standard No. 141.10: Securing Information Technology Assets, which states the following:

Agencies must develop, document and implement policies and procedures for the IT security program in Section 1 and the functional areas in Sections 2 through 11. Agencies may exceed these IT security standards based on the risk and complexity of the IT environment.

SCOPE

(1) The IT security policy applies to state of Washington executive branch agencies, agencies headed by separately elected officials, and institutions of higher education.

(2) These IT security standards apply to state of Washington executive branch agencies and agencies headed by separately elected officials, referred to as “agencies” throughout this document.

(3) Institutions of higher education shall develop standards that are appropriate to their respective missions and that are consistent with the intended outcomes of the OCIO to secure data, systems and infrastructure. At a minimum, higher education institutions' security standards shall address:
a. Appropriate levels of security and integrity for data exchange and business transactions.
b. Effective authentication processes, security architectures(s), and trust fabric(s).
c. Staff training.
d. Compliance, testing, and audit provisions.

Academic and research applications and infrastructure at institutions of higher education are exempt.

It is the intent of Big Bend Community College to take precautions to prevent revealing specific security policies, standards and practices containing information that may be confidential or private regarding BBCC 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 42.56.210 and 42.56.540). Policy Contact: Information Systems Manager

RELEVANT LAWS AND OTHER RESOURCES

RCW 42.56.210
RCW 42.56.540
RCW 43.88.160