

5250 INFORMATION TECHNOLOGY (IT) SECURITY POLICY

Original Date: 6/10/2003 Last Revision Effective: 5/21/2009

Policy Contact: Dean, Information Resources

POLICY

Bellevue College 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 Bellevue College policies pertaining to IT usage on campus, and complies with the [Washington State Department of Information Services \(DIS\) IT Security Audit Process](#).

The Bellevue College 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 Bellevue College community, with specific duties and responsibilities placed upon departments within information resources (IR). This policy applies to all campus facilities, equipment and services that are managed by the Bellevue College information resources 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 Department of Information Services (DIS) [Information Technology \(IT\) Security Policy](#) for Institutions of Higher Education, pursuant to [RCW 43.105.200](#), which states that, "in the case of institutions of higher education, the provisions of chapter 20, Laws of 1992, apply to business and administrative applications but do not apply to academic and research applications."

It is the intent of Bellevue College to take precautions to prevent revealing specific security policies, standards and practices containing information that may be confidential or private regarding Bellevue 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](#)).

IT Security

It is the sole responsibility of IR 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 Bellevue College.
- 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:

- Bellevue College will operate in a manner consistent with the goals of the [DIS IT security policy](#)

to maintain a shared, trusted environment within Bellevue College and within the Washington Community and Technical College (WACTC) system for the protection of sensitive data and business transactions.

- Bellevue College will maintain an IT security audit portfolio that includes comprehensive documentation of all processes, as required by the [Department of Information Services \(DIS\) IT Security Audit Process](#). Comprehensive documentation of all IT applications developed or purchased by the college after December 2002 will be included in this audit portfolio. This portfolio and all documentation related to any Bellevue College IT security policies will be maintained in the office of the Bellevue College IT security administrator.
- Bellevue College will submit annual written verification to the Washington state DIS verifying compliance with the processes and documentation of processes required by the [Department of Information Services \(DIS\) IT Security Audit Process](#).
- Bellevue College 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. Bellevue College will provide training to each employee in the security procedures for which they are responsible.
- Bellevue 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, Bellevue College will make appropriate updates as necessary.
- A compliance audit of this IT security policy will be conducted every three years and will be performed by knowledgeable parties independent of Bellevue College 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 Bellevue College 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 Bellevue College is dependent on secure IT to accomplish its critical business functions. Bellevue 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 Bellevue College IT security processes, policies, procedures, and practices, pursuant to [RCW 43.88.160](#) for compliance with this and the [DIS IT Security Policy](#).

RESPONSIBILITIES

Information Resources (IR)

Information Resources 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](#) and ([RCW 43.105.017\(3\)](#)). This written verification will include all revisions from previously submitted documentation, and will be submitted no later than October 6 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. Information Resources 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.

Technology Advisory Committee (TAC)

- The Technology Advisory Committee (TAC) is responsible for reviewing Bellevue College technology strategies and serving as a conduit for dialogue between IR and the campus regarding all technology policies and procedures. Membership of this group is representative of the campus, and supports the dean of information resources by advocating for and presenting the campus technology needs.

DEFINITIONS

Department of Information Services (DIS)

- The Washington State Department of Information Services (DIS).

Department of Information Services IT Security Policy

- Also called 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 Bellevue College 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.

Technology Advisory Committee (TAC)

- The Technology Advisory Committee (TAC) is a campus committee which is responsible for reviewing Bellevue College technology strategies, serving as a conduit for dialogue regarding technology policies and procedures. Membership to this group is representative of the campus and supports the dean of IR in representing the needs of all campus technology needs.

RELEVANT LAWS AND OTHER RESOURCES

[RCW 42.56](#)
[RCW 43.88.160](#)
[RCW 43.105.200](#)

REVISION HISTORY

Original 6/10/2003
Revision 5/21/2009

APPROVED BY

President's Staff