



IT Security Standard:

IT Security Administrator

Introduction

This standard defines the steps needed to implement Bellevue College Policy # 5250: Information Technology (IT) Security regarding the position and responsibilities of the Bellevue College Information Technology Security Administrator (ITSA). The standard will be reviewed on an annual basis or when changes are necessary.

Scope

This standard applies specifically to the duties and responsibilities of the ITSA and the qualifications for individuals holding the position.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

The Dean of IR has primary responsibility for management, coordination and oversight of IT at Bellevue College. Included in these responsibilities are:

1. IT portfolio management,
2. Disaster Recovery,
3. IT Security,
4. Public Records Privacy Protection, and
5. Communication and Telecommunications Architecture Standards.

Under the direction of that office, Bellevue College IT staff design, manage, and support the core services and business applications of the college. However, changes in the Washington state Department of Information Services (DIS) IT Security Policy, coupled with the rapidly expanding implementation of technology across campus have affected how the Dean's office and the institution are able to address and coordinate overall IT security and management activities.

Even the most detailed IT security strategy cannot be implemented without careful management of the resources used to put it into action and adequate communication with all technology users. Additionally, many aspects of instigating and managing the many security requirements set forth by the state make it imperative that sufficient oversight be built into the strategy, and that centralized administration and authority for applying IT security principles and practices be vested with a knowledgeable individual.

Without centralized management and vested authority for applying IT security uniformly across campus, Bellevue College runs the risk of a failure of the overall IT security strategy. The most significant threats related to a failure of the Bellevue College IT security strategy are:

1. Malicious and/or unauthorized modification of Bellevue College systems and networks
2. Malicious and/or unauthorized disclosure and/or modification of data
3. Malicious and/or accidental denial/loss of service
4. Theft of equipment or resources
5. Malicious and/or accidental damage to equipment or resources

Given the nature of Bellevue College's technology assets and the nature of threats to them, the primary risk associated with this failure of strategy is a lessened ability to protect Bellevue College systems and data, from either malicious acts or institutionalized carelessness. This failure can severely damage all Bellevue College technology resources and may include additional risks such as interruption of productive work, loss of revenue, failure to comply with state law, and significant loss of reputation.

Standard

A. General

1. Bellevue College has implemented an IT security program, articulating local policies and standards intended to bring the institution into compliance with state-level IT security requirements.
2. To manage and enforce this program, Bellevue College will maintain an IT Security Administrator position filled by a qualified individual assigned primary oversight of network and technology security and responsible for maintenance and implementation of the Bellevue College IT Security Program.
 - a. This position will report directly to the Dean of IR, assisting with all aspects of IT Strategic Planning, IT Portfolio Management, Disaster Recovery, Public Records Privacy Protection, and Communication and Telecommunications Architecture Standards, in addition to the primary IT Security responsibilities.

B. General Responsibilities

1. This position will fulfill all responsibilities for sustaining the Bellevue College IT security program as assigned by the Dean of IR, including:
 - a. Acting as direct advisor and consultant to the Dean with regard to IT security and related technological matters.
 - b. Working closely at administrative levels with supervisors and managers of various units and with IR technical supervisors and managers.
 - c. Making Bellevue College policy interpretations and decisions, including granting and documenting exceptions to policies and standards, with cause.
 - d. Auditing Bellevue College network, desktop and related technology resources to ensure compliance with IT security policy and DIS/ISB policies and standards.
2. Bellevue College security concerns and responsibilities cross internal organizational boundaries and, as such, the IT Security Administrator will:
 - a. Require strong support from Bellevue College management and staff to formulate and implement appropriate security.
 - b. Require a fairly broad background in areas of development practices, systems administration and operational practices, networking, and current trends in security.
 - c. Work to negotiate a balance between risk, risk mitigation, and business needs.
 - d. Work to integrate secure practices into business practices to assure acceptance by campus staff and users.
 - e. Have authority to set up, monitor, and enforce security rules and procedures.

- f. Make presentations to various levels of campus users, including President's Staff, regarding areas of responsibilities.

C. Specific Responsibilities

1. Ensure Bellevue College IT security compliance with DIS/Information Services Board (ISB) policies and standards.
2. Prepare for and coordinate Bellevue College and IR responses for official state IT Security Audits, regarding both the 3-year audit cycle and the annual review and reporting process.
3. Develop and maintain the Bellevue College IT security policies and standards.
4. Oversee IT disaster recovery planning, testing, assessment and execution.
5. Oversee the IT Security Training Plan.
6. Conduct in-house auditing of IT security processes and procedures.
7. Communicate on a daily basis with all IR service units that have hands-on responsibility for creating, supporting and maintaining IT security within their areas of stewardship.
8. Provide IT security standards/policy consultation and oversight for the whole campus, communicate with campus units regarding issues of IT security and security planning, and assist college staff and supervisors, as needed.
9. Publicize IT security policies, standards and responsibilities to both Bellevue College IT support personnel and general campus users, training them with regard to their individual responsibilities.
10. Represent IR IT security interests in various standing campus-level committees, such as the Facilities Universal Access Advisory Committee, i-BC Steering Committee, Web Advisory Committee, Technology Advisory Committee, the Risk Management Committee and the Emergency Preparedness Committee, as well as in ad hoc campus committees formed to address strategic technology planning and other campus-wide IT issues.
11. Actively present and represent IT security interests within IR, in groups such as the IR Leadership Team, the IT Management Team, the Network Server Group and others.
12. Coordinate with campus security and local law enforcement with regard to IT security matters.
13. Coordinate IR compliance with Bellevue College records retention policies, standards and expectations.
14. Ensure all issues related to these responsibilities are represented and addressed in the annual IT Strategic Plan.
15. In conjunction with college administrators and supervisors, enforce IT policies, standards and protocols, ensuring institutional and individual compliance.

D. Qualifications

1. An individual fulfilling these responsibilities ideally possesses high levels of specialized knowledge and skills, including:
 - a. A commitment to establishing and supporting a strong IT security environment at Bellevue College, while preserving the primary, service-oriented functions of IR.
 - b. Excellent communications skills and the ability to work with a diverse group of staff, managers and administrators within the sundry IR units having primary responsibility for wide-spread, hands-on establishment and monitoring of IT security.
 - c. An ability to work collaboratively and effectively with the disparate needs, skill levels and expectations of a variety of campus units, showing the individual is comfortable, productive and effective in any group situation.
 - d. Good analytical skills, the ability to identify key security issues quickly, and the capacity to collaboratively develop strategic solutions which are effective and feasible for the campus while maintaining the integrity of the college's core mission and values.

- e. An innovative and flexible leadership style, showing willingness and an ability to build consensus when possible, while still working within the fairly rigid institutional, state and federal guidelines.
- f. An ability to compose written materials clearly and concisely, including policies, standards, and correspondence, all of which clearly articulate complex compliance requirements to both technical and non-technical employees.
- g. A minimum 3 years combined education and/or experience in IT security is required. Additional experience in law enforcement or investigative and legal fields is desirable.
- h. An ability to fulfill the “*Essential Functions*,” and possession of the “*Knowledge, Skills and Abilities*” identified in the Bellevue College IT Security Administrator position description (Appendix B).

E. Documentation Procedures

1. The Bellevue College Information Technology Security Administrator (ITSA) will be responsible for creating and updating most policies and standards developed as a part of Bellevue College’s IT security program.
 - a. These documents will adhere to campus expectations for written documentation and will be processed through the review procedure identified in the IT security standard regarding the Bellevue College “*Security Program and Strategy*” and in Bellevue College policy #1250: “*Formulation and Issuance of College Policies*.”
2. In addition, the ITSA will have primary responsibility for maintaining all written records and archives pertaining to the Bellevue College IT Security program.

F. Personnel Actions

1. Procedures for hiring and annually evaluating any individual assigned as the Bellevue College IT Security Administrator will adhere to standard Bellevue College Human Resources policies, and follow the requirements of the Bellevue College IT security standard addressing “*IT Support Personnel*.”

Appendix A – References

1. Bellevue College Policy #5250: *Information Technology (IT) Security*
2. Bellevue College Policy #1250: *Formulation and Issuance of College Policies*
3. Bellevue College IT Security Standard: *Security Program and Strategy*
4. Bellevue College IT Security Standard: *Employee Security Training*
5. Bellevue College IT Security Standard: *IT Support Personnel*
6. Department of Information Services (DIS) IT Security Policy
7. Bellevue College IT Disaster Recovery and Business Resumption Plan
8. Bellevue College IT Strategic Plan

Effective Date: June 10, 2005
 Date Last Modified: April 12, 2009

Appendix B – Bellevue College Administrative/Exempt Position Description:

Information Technology Security Administrator

JOB SUMMARY:

Under the direction of the Dean of Information Resources (IR), the Information Technology Security Administrator (ITSA) manages, coordinates and oversees specific areas of the Dean's responsibilities, delegated to include all aspects of the Bellevue College IT Security Program, IT Strategic Planning, IT Portfolio Management, Disaster Recovery, Public Records Privacy Protection, and Communication and Telecommunications Architecture security standards.

As an expert, professional level technology specialist, the IT Security Administrator will be assigned primary oversight of network and technology security, will address and coordinate overall IT security and management activities across campus, and will be a direct expert-level advisor and consultant to the Dean and other Bellevue College executives and administrators with regard to IT security and related technical matters.

ESSENTIAL FUNCTIONS:

- **Administrative**
 - Provide technical and organizational leadership for the Bellevue College campuses, offering centralized management and authority regarding IT security principles and practices uniformly across campus.
 - Manage the Bellevue College IT Security program. This includes:
 - Develop, implement and maintain the Bellevue College IT security policies and standards.
 - Set up, monitor, and enforce Bellevue College IT security rules, standards, and procedures.
 - Make policy interpretations and decisions, including granting and documenting policy exceptions with cause.
 - Instigate and manage college adherence to the security requirements set forth by the state.
 - Prepare for and coordinate Bellevue College and IR responses for official state IT Security Audits, regarding both the 3-year audit cycle and the annual review and reporting process.
 - Maintain all written records and archives pertaining to the plan and all security activities.
 - Oversee IT disaster recovery and business continuity planning, testing, assessment and execution, defining off-site disaster recovery back-up requirements for databases and system files.
 - Coordinate IR compliance with Bellevue College records retention policies and standards.
- **Technical**
 - Provide day-to-day network and security support for mission-critical and infrastructure-related systems. This includes performing hands-on administration of all aspects of network, server and client security, including:
 - Create and maintain secure network log-in accounts for all campus users.
 - Administer security rights for approved system accesses.
 - Assist in the design of network architecture and structure.
 - Security software testing, installation and administration.
 - Network and e-mail server and system scanning and monitoring,
 - Act as a member of the Network Server Group when responding to security threats, with responsibilities for response to prevention, evaluation, detection, resolution, and remediation of security threats.

- Serve as a technical mentor, coach and trainer to the Network Server Group, Desktop Support personnel and others, acting as an expert security resource for those involved in day-to-day technical support positions and for their supervisors.
- Conduct hands-on technical audits of the Bellevue College networks, desktops and related technology resources to support data security management and to ensure individual and institutional compliance with Department of Information Systems (DIS)/Information Services Board (ISB) policies and standards.
- **Consultative**
 - Provide IT security standards/ policy consultation and oversight for the whole campus, communicating with campus units regarding issues of IT security and strategic security planning—assisting executive management, administrators, supervisors, and college staff.
 - Act as security consultant for internal IR groups such as Computing Services, the IR Leadership Team, the IT Management Team, the Network Server Group and Technology Development and Support Services, assisting with security problem resolution.
 - Communicate on a daily basis with all IR service units that have hands-on responsibility for creating, supporting and maintaining IT security within their areas of stewardship.
 - Participate in network strategic and day-to-day planning meetings as a consulting member of the Network Server Group.
 - Serve as both a management advisor/consultant and technical resource, enhancing and maintaining secure on-going operations of all applications (mainframe, client/server, web, microcomputer, etc.) within the Bellevue College network.
 - Actively represent IR management and IT security interests:
 - By participating in various standing campus-level committees, such as:
 - ❖ The Facilities Universal Access Advisory Committee,
 - ❖ The i-BC Steering Committee,
 - ❖ The Web Advisory Committee,
 - ❖ The Technology Advisory Committee,
 - ❖ The Risk Management Committee,
 - ❖ The Emergency Preparedness Committee, and
 - ❖ Any ad hoc campus committees formed to address strategic technology planning and other campus-wide IT issues.
 - By making presentations regarding areas of responsibility to various levels of campus users (including President's Staff), and to entities outside Bellevue College.
 - By coordinating with campus security and local law enforcement regarding IT security matters.
 - Ensure all issues related to IT security are represented and addressed in the annual IT Strategic Plan and IR work plans.
 - Work closely with college administrators, supervisors, and with IR technical managers, to enforce IT policies, standards and protocols.
 - Administer the IT Security Training Plan for both Bellevue College IT support personnel and general campus users, publicizing the security program and training individuals with regard to the IT security policies, standards and their individual responsibilities.

KNOWLEDGE, SKILLS, AND ABILITIES:

- A Bachelor's degree in Information Technology, Information Management, or Information Security; or a minimum 3 years background, education and experience in Information Systems or IT Security management. Additional experience in law enforcement or investigative and legal fields is desirable.
- An innovative and flexible leadership style, showing willingness and ability to build consensus when possible, while working within fairly rigid state and federal guidelines. This is demonstrated by a

commitment to establishing and supporting a strong IT security environment at Bellevue College, while preserving the primary, service-oriented functions of IR and the college.

- Excellent understanding of federal, state and local legal and/or regulatory requirements for higher education as it applies to information security and data privacy.
- **Expert technical skills:**
 - Expert level knowledge of technical and security issues regarding local and wide area networks, including server/client security architecture and network security risk analysis.
 - Network administration skills, including systems and user administration, email systems administration, server/client virus and malware scanning, and threat incident response.
 - Experience with information security technologies and technical network processes in the areas of prevention, evaluation, detection, resolution, and remediation of threats.
 - Broad technical understanding of all aspects of the use of technology in addition to network administration skills, including applications development practices and desktop support systems, practices and administration.
- **Advanced business knowledge and skills:**
 - The ability to translate technological options into business terms, understanding and managing the impact of technology security on college business practices.
 - Skills to interact with executive management to create secure technology solutions to mission critical business problems.
 - Able to work with all levels of institutional management regarding technology security, campus business resumption, technology disaster recovery and technology audit best practices.
 - Solid analytical skills that show the ability to define, collect and analyze data, establish facts, draw valid conclusions, and make fact-based decisions.
 - Must have the ability to identify key security issues quickly and have the capacity to collaboratively develop strategic solutions that are effective and feasible for the campus, while maintaining the integrity of the college's core mission and values.
- **Exceptional communications skills:**
 - Capable of composing written materials concisely, including policies, standards, and correspondence, all of which clearly articulate complex compliance requirements to both technical and non-technical employees.
 - Able to communicate effectively and comfortably with individuals, and in any group, at all levels in the organization, including executive management.
 - Able to work with a diverse group of staff and administrators within the many IR units having primary responsibility for hands-on management of IT security.
 - Proficient at working collaboratively with the disparate needs, skill levels and expectations of campus units outside IR.