

IT Security Standard:

Intrusion Detection and Incident Response

Introduction

This standard defines the steps necessary to implement the Bellevue College IT Security Policy for the detection and handling of computer system security incidents. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to Bellevue College system administrators responding to identified and/or suspected security breaches and defines specific procedures for addressing such incidents.

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 goal of detecting and handling a security incident is to assure services are provided as incident-free as possible and restored as quickly as possible. Incident detection is a positive proactive step to recognize and respond appropriately to incidents as soon as detected/reported. However, incident response is, by its very nature, reactive. Risks and business impacts will center on the trade-offs between restoring services quickly, and the time required to understand the full nature and scope of the incident.

Standard

A. Introduction

1. In essence, all Bellevue College IT security policies and standards are in place to facilitate compliance with Bellevue College Policy #5250 – *Information Technology (IT) Security*, and to prevent inappropriate and unauthorized use of Bellevue College computers, systems, and networks. This standard assumes compliance with all of those policies and standards, and expects all system administrators to be familiar with them.
2. In addition, system administrators will be familiar with this standard and will stay apprised of any new trends in security management and/or current vulnerabilities. This will enable them to prevent/avoid incidents as much as possible and to react with the appropriate response. The following are fairly standard and thorough guidelines for detecting and handling suspected security incidents.

3. As a general rule, Bellevue College is not inclined to pursue criminal investigation or prosecution, but rather will focus on the quick restoration of services. It is still valuable, however, to perform an investigation to identify the attack vector, the extent of the damage, and other hosts who might have been either originators or later victims in any attack.

B. Incident Detection

1. The initial point of contact for any suspected security breaches is the system administrator for the affected Bellevue College system. The Bellevue College IT Security Administrator and/or the Dean of Information Resources and the Director of Computing Services will be notified immediately of a suspected incident. Systems administrators should not hesitate to follow the appropriate steps detailed herein at the first indication of security breach.

2. Monitoring and Preventive Measures

- a. All system monitoring, logging and log review measures described in the Bellevue College IT Security Standard addressing "Windows Base System Configuration" will be followed on a daily basis on individual server-class computers. Periodic system scan and assessment measures defined in the same standard will be monitored as directed. Software tools such as Multi-Router Traffic Grapher, Languard, and the Microsoft Operations Manager will be used to simplify and facilitate this monitoring.
- b. The primary responsibility for monitoring and for all preventive measures rests with the system administrator for each networked server system.
- c. Events logs will be configured to monitor all network, server, and computer activities. Systems administrators will check these daily to determine if there are any unusual connections to Bellevue College systems.
- d. Twice weekly (more if a known threat exists) SMTP, IIS and FTP logs will be checked to identify any unusual occurrences for that week.
- e. All Internet Security and Acceleration (ISA) server logs will be checked weekly for any port probes.
- f. Port scans for known FTP, WWW, and SMTP ports will occur at different times during the week to ensure no rogue servers are being operated on the network.
- g. Daily virus scans will be configured in accordance with the Bellevue College IT security standard addressing "Virus Protection."
- h. Probes for known Trojans on the network systems will be made quarterly. If new information on a specific Trojan is released, the System Administrator will do specific scans on those affected ports to determine risk levels.
- i. Outbound traffic from all Bellevue College switches will also be monitored and checked daily to determine any unusual and/or unexplainable traffic spikes.
 - i. If a particular workstation is broadcasting a great deal of traffic, the processes running on the system will be checked.
 - ii. The system will be examined to determine if there is anything unusual about the configuration or setup of the system.
 - iii. If appropriate, the Incident Response procedures outlined in this standard will be followed.
- j. If a particular external IP address has been compromised, an attempt to track back to the point of origin will be made, the information recorded, and appropriate steps followed as outlined in this standard.

3. Indications of a Potential Compromise

- a. The initial suspicion or identification of a compromised computer system is not always easily apparent. There are a wide range of behaviors that might serve as problem indicators, but in most cases they are not definitive. These factors might include:
 - i. Unusually poor system performance.
 - ii. Unusually high and unaccounted for network traffic.

- iii. Unusual open network ports.
 - iv. Unusual running programs.
 - v. Unusual programs installed on disk.
 - vi. Unusual blue screen, CD drawer opening and closing, mouse moving around screen.
 - vii. Sluggish or non-responsive network access (Web sites do not display quickly or at all).
- b. While none of these indicators is solid evidence of a compromised computer, any one of them could be the first sign of a problem. If a user notices these types of behaviors for a computer being used, the Help Desk (x3457) is to be contacted so the behavior can be referred to the appropriate system administrator.

C. Incident Response

1. As no two incidents are alike, each step listed may not apply to each event. Before dropping any step, the responding technical support personnel will be sure it is appropriate to alter the procedures and that the elimination of one step will not jeopardize later steps in the investigation.

2. General Guidelines

- a. Notify the appropriate people for the incident. This will include at least the Systems Administrator for the suspected device, the appropriate IR supervisor, the Bellevue College IT Security Administrator and/or the Dean of Information Resources. It may also include technical support staff, management and others, as necessary. Identify all of the key players as early as possible.
- b. The system administrator for the suspected device will take the lead in handling the incident and in instructing other staff regarding the immediate response needed. Upon resolution of the incident, a written report will be made to the Bellevue College IT Security Administrator, the Dean of Information Resources, and the appropriate IR supervisor.
- c. Document everything. Consider taping your comments. Note who did what, when, and why.
- d. Keep your head. Resist the tendency to overreact or panic. Methodically follow this standard.
- e. When communicating with others working on the incident, use communication such as telephone, fax and face-to-face communication instead of communicating across the potentially compromised system. The attacker may be able to "listen" in.
- f. Stay in constant communication across teams and with other impacted individuals.
- g. Avoid restarting the computer, logging on and off, or otherwise inadvertently starting malicious code. Remember, the programs on a compromised computer cannot be trusted.

3. Stage 1 – Make Initial Assessment

- a. Ensure incident is not a false alarm.
- b. Examine all system and security audit logs for unusual activity, absence of logs or gap in logs.
- c. Look for attack tools (password cracking tools, Trojan horses, etc.)
- d. Scan network for known compromises.
- e. Check for unauthorized applications or services configured to start automatically.
- f. Examine accounts and groups for increased privilege or unauthorized group members.
- g. Check for unauthorized processes and services.
- h. Match compromised system performance against baseline system performance.
- i. Attempt to make a preliminary assessment of the nature, purpose, and extent of the compromise.

- j. Assign an initial priority level (i.e., high, moderate, low).
 - k. Determine if evidence will need to be preserved for a potential criminal investigation.
 - l. Communicate the incident to appropriate personnel. This may, depending on the nature of the incident, include Bellevue College management and law enforcement, the State Board for Technical and Community Colleges – Information Technology unit (SBCTC-IT) and state level response agencies such as Washington Computer Incident Response Center (WACIRC).
- 4. Stage 2 – Protect Evidence**
- a. While chain-of-custody may not be essential in most incidents, creating a good system backup will be performed for any significant compromise. Some containment steps (such as Step 3) may be done together with this step.
 - i. As early as possible in the incident response, back up systems with media never before used.
 - ii. If possible, back up the entire system, including logs and system state.
 - iii. If critical, maintain documented chain-of-custody for evidence collected.
 - iv. Secure evidence and document who collected, how, when, and who had access to it.
- 5. Stage 3 – Contain the Damage and Minimize Risk**
- a. Depending on severity and, in accordance with Bellevue College Policy #5250 – Information Technology (IT) Security, isolate the affected systems by taking them offline.
 - i. This will be done by physically removing the network connection, isolating the system in a private network, or shutting the system down.
 - ii. Shutting the system down will be the last resort if the system is compromised as it may be difficult to track the root of the problem once it has been restarted.
 - b. Look for evidence of compromise on neighboring systems.
 - c. Change passwords on affected systems
- 6. Stage 4 – Identify Type and Severity of Compromise(s)**
- a. Determine the type of attack and how it was accomplished.
 - b. Perform a system and network vulnerability analysis on the system to identify if there are other related or overlooked vulnerabilities to be considered.
 - c. Determine probable intent of attack (specifically directed at Bellevue College, automated attack, information gathering or probing).
 - d. Identify all systems involved in the attack. Repeat containment steps if additional compromised systems are identified.
 - e. Reevaluate and, if necessary, reassign priority level to event.
- 7. Stage 5 – Notify External Agencies**
- a. Update the Bellevue College IT Security Administrator, the Dean of Information Resources, and appropriate IR IT support management to ensure they have an accurate understanding of the incident and its status.
 - b. After consulting with Bellevue College management, notify legal counsel, who may notify local and/or federal law enforcement, as appropriate.
 - c. Notify the State Board for Technical and Community Colleges – Information Technology unit (SBCTC-IT) and state level response agencies such as Washington Computer Incident Response Center (WACIRC), if appropriate.
 - d. Notify other appropriate agencies, such as the CERT Coordinating Center (http://www.cert.org/reporting/incident_form.txt), as appropriate.
- 8. Stage 6 – Recover Systems**
- a. Determine whether damaged systems should be recovered with a complete reinstall or from backup.

- b. Locate and validate most recent non-compromised backups or recovery media.
- c. Recover the system.
- d. Validate functionality and match system performance against historical baselines.
- e. Verify that the vulnerability (ies) that caused the incident are adequately addressed.
- f. Determine if it is acceptable to bring the computer systems back online.
- g. Monitor for repeat attack and for possible mis-configuration due to the steps taken during the containment process.

9. Stage 7 – Compile and Organize Incident Documentation

- a. Compile all notes and records into a comprehensive security breach activity log.
- b. Distribute documents to incident participants for review and approval, as appropriate.
- c. Review cause of breach and improve defense to prevent it and related attacks in the future.
- d. Prepare report to management and other stakeholders to explain how the event occurred, the cause of the breach, and how it will be prevented in the future, as required by the impact of the incident.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

- 1. Permanent loss of computer use privileges;
- 2. Denial of future access to Bellevue College IT resources;
- 3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
- 4. Dismissal from the college; and/or
- 5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

- 1. SANS; *Computer Security Incident Handling Step by Step*; Version 1.5; SANS, 1998
- 2. SBCTC-IT Security Standard—*Security Incident Handling*
- 3. Bellevue College Policy #4400, *Acceptable Use of State Resources*
- 4. Bellevue College Policy #5000, *Acceptable Use of Bellevue College Computers*
- 5. Bellevue College Policy #5150, *Acceptable Use of Bellevue College Networks and Systems*
- 6. Bellevue College Policy #5250 – *Information Technology (IT) Security*
- 7. Bellevue College IT Security Standard: *Windows Base System Configuration*
- 8. Bellevue College IT Security Standard: *Macintosh Base System Configuration*
- 9. Bellevue College IT Security Standard: *Virus Protection*
- 10. Bellevue College IT Security Standard: *Windows Server System Configuration*
- 11. Bellevue College IT Security Standard: *Macintosh Server System Configuration*

Effective Date: July 2003
Date Last Modified: April 12, 2009