

## *IT Security Standard:*

# **Network Device Configuration and Management**

### **Introduction**

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding the specific procedural and configuration elements for management of network infrastructure devices under Bellevue College control. The standard will be reviewed on an annual basis or when changes are implemented.

### **Scope**

This standard addresses the support of all network devices, generally including such things as routers, bridges, switches, firewalls, hubs, and the interconnecting cables, but also extending to computers on the network themselves. This standard also addresses the tools and protocols used for network management.

Bellevue College is principally responsible for the management of its network at all Bellevue College facilities. The K20 border-router on the Bellevue College main campus is managed by the State Board for Technical and Community Colleges – Information Technology unit (SBCTC-IT). The T1 Network Interface Units (NIU) at Bellevue College are leased facilities, owned and managed by an outside vendor. The PIX Firewall will be maintained by Bellevue College under advisement of SBCTC-IT. The Private Business Exchange (PBX) system is owned and managed by Bellevue College, and maintained by an outside vendor under a service contract agreement. Physical access to all network devices on Bellevue College campuses and facilities by both Bellevue College and non-Bellevue College employees will be in accordance with the Bellevue College IT Security Standard addressing “Physical Security.”

Myriad Bellevue College IT security policies and standards address specific components of the network and processes regarding their management. This standard is intended to supplement those standards, not supersede them.

### **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 network components within the scope of this standard are critical infrastructure to the daily business and operations of Bellevue College. There remains some possibility, under severe conditions, that

Bellevue College business (administrative, instructional, and public service) functions could nearly halt with significant network disruption.

Given the high level of dependence on the network, the most significant threats are:

1. Malicious and/or unauthorized access to data
2. Malicious and/or unauthorized modification of data
3. Accidental modification of data (e.g., while performing support)
4. Theft of equipment or resources
5. Malicious and/or accidental damage to equipment or resources
6. Malicious and/or accidental denial/loss of service

Given the nature of the asset and the nature of the threat, the primary risk associated with the networking infrastructure is loss of service. This loss of service could have associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and a loss of reputation. In the event of damaged or stolen equipment, risks may also include the replacement cost of that equipment.

Secondary to these threats is the potential for inappropriate use of the resource. This can include such things as excessive bandwidth use, uses inconsistent with the Bellevue College mission, uses that are in violation of the Bellevue College Acceptable Use policies, or are in violation of state and/or federal law.

## Standard

### **A. Purchasing and Installing Equipment to the Bellevue College Network**

1. The request to purchase any technology hardware that will be or could potentially be connected directly, or indirectly, to the Bellevue College network requires prior approval from the Dean of Information Resources, or an authorized designee.
2. Appropriate IR staff, or designees, are the only individuals authorized to attach equipment to the Bellevue College network.

### **B. Password**

1. First level passwords (passwords used to establish initial access to the device) will be set and encrypted, if possible.
2. Second level passwords (passwords used to access sensitive device functions) will be stored in a MD5 hash format, or better, whenever possible.
3. Choice of secure passwords and management of those passwords will adhere to the Bellevue College IT Security Standards addressing "Password Management" and "Password Management Exceptions."
4. Backup copies of configuration files which contain clear text passwords will be protected from unauthorized access. These configuration files will be maintained on a secure server location accessible only by authorized personnel.
5. Configuration files will be backed up to the system's tape on the server's regular backup cycle.

### **C. Console and Terminal Access**

1. Clear text protocols will be avoided and be completely phased out over time.
2. Physical access to the device will be tightly maintained in accordance with the Bellevue College IT Security Standard addressing "Physical Security."
3. Remote access protocol will, wherever possible, support strong authentication.
4. Idle connection timeouts will be set to low, but reasonable, values (e.g., 600 seconds).
5. Remote access to these devices will be restricted to a small number of computers on a secure internal network.

6. A login banner will clearly state that the systems are monitored, that unauthorized access is not allowed, and will not provide information as to equipment type, operating system type, or version. (Refer to the Bellevue College IT Security Standard addressing "Login Banner")

#### **D. Services**

1. All unused network connectivity services on configurable devices will be disabled.
2. All small services will be disabled.
3. The finger services will be disabled.
4. The bootp services will be disabled unless required by older devices to make IP reservations. Network administrators will document these exceptions.
5. Secure Socket Layer (SSL) enabled Hypertext Transport Protocol Secure (HTTPS) will be used for monitoring devices; if HTTPS is not supported by the device, HTTP may be used as a fallback. Management of devices via HTTP is strongly discouraged. If HTTP device management can be disabled independently of HTTPS device monitoring, it will be. Telnet within the secure network may also be used.
6. All network devices featuring syslog capability will be configured to use syslog for centralized log management. Network-enabled printers are exempt from this requirement.
7. All network devices that support time synchronization will be maintained via Network Time Protocol (NTP) and will be configured to retrieve time from one of the Domain Control Servers or a similarly reliable and secure time source.
  - a. NTP updates will be authenticated.
  - b. The choice and management of authentication keys will follow the criteria defined in the Bellevue College IT Security Standard addressing "Password Management."
  - c. The same key will be used on all devices in the network.
8. Use of Simple Network Management Protocol (SNMP- also implies SNMPv2 or SNMPv3) will comply as follows:
  - a. Use of default community strings will be limited. Community strings, being effectively a password, will be chosen following the same criteria as defined in the "Password Management" standard.
  - b. All internal network devices will be configured to use the same community string.
  - c. All external border routers over which Bellevue College has control will use unique community strings.
  - d. SNMP updates will be disabled.
  - e. Access Control Lists (ACL) to restrict access to device via SNMP, will be defined to allow access from a secure Bellevue College network, or from SBCTC-IT to border routers at Bellevue College.

#### **E. Network Changes**

1. No one (including employees, students and vendors) will implement changes to the Bellevue College Network topology, fiber optic backbone, or horizontal data and voice cabling without the knowledge and approval of the IR Dean or an authorized designee.
  - a. Those who are allowed to make changes to this basic infrastructure include members of the Network Servers Group (NSG) and/or authorized vendors working on specified changes approved by the Dean.
  - b. This will include all network equipment, network devices, and cabling between/within the Phone Vault, Server rooms, Intermediate Data Facility (IDF) closets and cabinets, up to and including wall data/voice jacks.
2. The NSG will document the physical and logical connections between network components, down to and including room ports and access points. Other IT support

personnel may assist in this endeavor. This documentation may be any combination of printed and electronic diagrams and inventory databases.

- a. Hard copies of network documentation will be physically stored in a secure location and protected from unauthorized access.
  - b. Electronic copies will be stored on secure servers or on physical media that are physically secured just as are hard copies.
  - c. Verification of installation of these network components, including cross-referencing against inventory records, will take place whenever maintenance is required, or annually, whichever occurs first.
3. The NSG will establish procedures for changing end-port assignments and/or adding computing workstations or devices to the network.
- a. IT support personnel will ensure that only authorized workstations or devices are connected to the network and that all IT security and IR management procedures pertinent to the use of the equipment on the network are followed.
    - i. Installations of Bellevue College-owned computers and devices will be tracked via purchasing records and electronic inventory.
    - ii. Non-Bellevue College owned computers and devices will be added to the tracking mechanism if they are authorized to connect to the network.
  - b. No component may be added to any Bellevue College network, down to and including any workstation or end-user device, without careful testing of component and verification of the impact of said connection on the existing network.

## Device Specific Configurations

### ***A. Router Access Control Lists (ACL) for the K20 Border Router***

1. Basic access controls will be in place to provide rudimentary protection of the device itself, as well as protecting both the internal and the external networks from each other.
2. Basic device protection will include allowing SNMP queries only from a defined secure SBCTC-IT network. Remote login access will be restricted to connections originating from a secure internal SBCTC-IT network. Bellevue College provides only Layer1 maintenance to the K20 Border Router present at the Bellevue College campus.
3. Basic network protection will include blocking directed broadcasts to guard against being used as a denial-of-service attack relay.
4. To prevent egress spoofing, ACL(s) will verify that all outbound packets have a source address that is from an internal network; if not, it will be logged and dropped.
5. To prevent ingress spoofing, ACL(s) will verify that all inbound packets have a valid source address. Address types that will be dropped and logged are:
  - c. private address range (as defined by the Internet Assigned Numbers Authority [IANA]),
  - d. addresses on the internal network,
  - e. local broadcast address,
  - f. loopback address (127.0.0.0/8), and
  - g. 0.0.0.0.
6. Source routing will not be allowed.
7. SNMP outbound from the college's network will be blocked at the K20 border router.
8. **Note:** this device is controlled by SBCTC-IT.

## **B. Configurations Specific to the Bellevue College PIX Firewall**

1. The ACL's defined on the Private Internet Exchange (PIX) firewall to protect the various DMZ and internal networks are beyond the scope of this standard. (Refer to the Bellevue College IT Security Standard addressing "Firewall Change Management")
2. ICMP access beyond the DMZ (onto the internal network) will be restricted to the bare minimum to allow internal authorized personnel to troubleshoot network connectivity.
3. Floodguard will be enabled to assure a console login is available even under high loads, such as a DoS attack.
4. The various protocol fix-up routines will be used with care as they can break some legitimate implementations of those protocols (SMTP as an example) or can generate huge amounts of log information (HTTP, SMTP for example).
5. Network Address Translation (NAT) will not be used.

## **C. Network Management Stations**

1. Network monitoring with tools on any dedicated network management stations will be conducted only by authorized network personnel. Configuration of such stations will follow the network device security services standard, as presented above.

## **D. Configuration Specific to Wireless Networking**

1. This is covered in the Bellevue College IT Security Standard addressing "Wireless Network Configuration and Management."

## **E. Virtual Private Networks (VPN) and IPSec**

1. Bellevue College does not have devices connected to external networks either directly or through an extranet/VPN connection that is connected to or part of the State Governmental Network (SGN). If Bellevue College does determine that it would be feasible and cost-effective to such a connection within the SGN, all rules, standards and guidelines as prescribed by DIS/ISB will be followed and the DIS Senior Technology Management Consultant will be contacted.
2. Bellevue College does not operate a token-based VPN solution. If Bellevue College does determine that it would be feasible and cost-effective to implement a token-based VPN solution, all rules, standards and guidelines as prescribed by DIS/ISB will be followed and the DIS Senior Technology Management Consultant will be contacted.
3. The remaining aspects of the use of VPN at Bellevue College are covered in the Bellevue College IT Security Standard addressing "Remote Access to Bellevue College Systems."

## **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

**Note:** All IT security standards identified below as references have components governing configuration and change management related to the specific network area addressed by the standard and should be consulted before changes to the addressed systems or security program components are made.

1. SBCTC-IT IT Security Standard - Network Device Configuration, February 20, 2003
2. Washington State DIS Security Guidelines, February 6, 2002
3. SBCTC-IT IT Security Standards- Physical Security, CIS, 2002
4. Bellevue College IT Security Standard: [byRequest Configuration](#)
5. Bellevue College IT Security Standard: [Data and Program Backup](#)
6. Bellevue College IT Security Standard: [Disaster Recovery](#)
7. Bellevue College IT Security Standard: [DNS Configuration](#)
8. Bellevue College IT Security Standard: [Electronic Mail Configuration](#)
9. Bellevue College IT Security Standard: [Firewall Change Management](#)
10. Bellevue College IT Security Standard: [HP Administrative System Access](#)
11. Bellevue College IT Security Standard: [Internet Software Security](#)
12. Bellevue College IT Security Standard: [Intrusion Detection and Incident Response](#)
13. Bellevue College IT Security Standard: [Login Banner](#)
14. Bellevue College IT Security Standard: [Macintosh Base System Configuration](#)
15. Bellevue College IT Security Standard: [Macintosh Server Configuration](#)
16. Bellevue College IT Security Standard: [MPE System Configuration](#)
17. Bellevue College IT Security Standard: [Network Data Storage](#)
18. Bellevue College IT Security Standard: [Network Printer Configuration](#)
19. Bellevue College IT Security Standard: [Network Printer Configuration Exceptions](#)
20. Bellevue College IT Security Standard: [Password Management](#)
21. Bellevue College IT Security Standard: [Password Management Exceptions](#)
22. Bellevue College IT Security Standard: [Phone System Configuration](#)
23. Bellevue College IT Security Standard: [Physical Security](#)
24. Bellevue College IT Security Standard: [Remote Access to Bellevue College Systems](#)
25. Bellevue College IT Security Standard: [Security Privileges](#)
26. Bellevue College IT Security Standard: [Software Management](#)
27. Bellevue College IT Security Standard: [SSH Configuration](#)
28. Bellevue College IT Security Standard: [Technology Purchasing and Logistics](#)
29. Bellevue College IT Security Standard: [Use of Bellevue College Resources Off-Campus](#)
30. Bellevue College IT Security Standard: [User Management](#)
31. Bellevue College IT Security Standard: [Non-Employee Access to Bellevue College Systems and Data](#)
32. Bellevue College IT Security Standard: [Virus Protection](#)
33. Bellevue College IT Security Standard: [Web Servers](#)
34. Bellevue College IT Security Standard: [Windows Base System Configuration](#)
35. Bellevue College IT Security Standard: [Windows Server Configuration](#)
36. Bellevue College IT Security Standard: [Wireless Network Configuration and Management](#)

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