

IT Security Standard:

MPE Configuration

Introduction

This standard defines specific procedural and configuration elements for managing MPE/iX systems in support of Bellevue College policy # 5250: Information Technology (IT) Security. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the specific steps needed to implement MultiProgramming Executive (MPE) System Configuration for the college's HP 3000 system. This standard is in compliance with the Shared Expectation Agreement between Bellevue College and the State Board for Technical and Community Colleges – Information Technology unit (SBCTC-IT)(formally the Center for Information Services [CIS]), a copy of which is provided in Appendix C of the Bellevue College IT Security Standard addressing "HP Administrative System Access."

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 computing resources within the scope of this standard are critical infrastructure to the daily business and operations of Bellevue College. With disruption to these services, the business functions (administrative services) of Bellevue College nearly halt.

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

1. Malicious and/or unauthorized access, user privilege level or system privilege level.
2. Malicious and/or unauthorized disclosure of protected information
3. Malicious, unauthorized and/or fraudulent modification of data
4. Denial of service
5. Interruption to electrical power
6. Malicious and/or accidental physical damage
7. Theft of computer resources

Given the nature of the asset and the nature of the threat, the primary risk associated with the MPE server is unauthorized access to the data. This unauthorized access could result in disclosure of protected information, the commission of fraud, or (illegal) use of information for personal gain. These

threats have associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, litigation, and a loss of reputation.

Standard

A. Introduction

1. This section describes the actual business practices covered by this standard including system building and maintenance, system configuration, and general management.

B. System Build and Maintenance

1. Initial Build

- a. The initial system build will be performed with the computer system disconnected from the network or on a network completely disconnected from the Internet and production networks. It will only be connected to the production network once it has been fully built and security hardened.
- b. System builds will be performed with the latest version of the OS that is supported by the hardware and application vendors.
- c. The most recent recommended power patch will be installed. All applicable security patches will be installed.
- d. All services in inetd will be disabled. If some of these services are needed to support the business use of the processor, they will be added back after the hardening process is complete. If inetd is to be used, then the job will be configured to log connections and the log will be reviewed daily.
- e. Only necessary and appropriate devices and jobs will be enabled/streamed during the startup process. This will vary by specific platform to some degree, but the objective will be to disable all but the bare minimum jobs.
- f. All users with "system management" capability will be required to have MPE passwords in addition to a Security/3000 password. All other users will be required to have at least Security/3000 passwords.
- g. Login User Defined Controls (UDCs), as well as other UDCs that control or restrict access to accounts and logins or may contain sensitive data, must have NOBREAK, NOLIST, and NOHELP enabled.
- h. The file systems will be scanned to assure no unnecessary files, groups, or accounts have System Manager (SM) or Privileged Mode (PM) privileges, or are world writable (that is, are writeable across accounts).
- i. If SNMP is to be run on the processor, the configuration file will be updated to disable the write community string, set a random-read community string, and to restrict the IP addresses that can communicate to the device via SNMP.
- j. NMMGR will be configured to allow the smallest reasonable number of networks to communicate with the HP3000.

2. Software Patches and Updates

- a. Security patches will be installed as quickly and safely as possible for all OS and application security vulnerabilities.
- b. Recommended patches will be regularly installed on the computer.
- c. Upgrades to new OS and application versions will be performed based upon a business need only after security issues have been examined.

3. Physical Security

- a. Bellevue College's MPE server is located in the Information Resources server room. This facility provides keypad access control, climate control, and appropriate fire suppression.

C. System Configuration

1. Services

- a. While many of the "standard" Internet services will run on the HP3000 under MPE, most of those services are not necessary or are incompatible with the purpose of the processor. Minimal network services will be allowed for inbound connections.
- b. Standard MPE networking protocols will be configured. These protocols include: Remote File Access (RFA), Remote Process Management (RPM), Virtual Terminal (VT), Network File Transfer (NFT), NS Information Request (NSIR).
- c. Additional protocols will be configured to support SBCTC-IT developed applications. These protocols include: Web Transaction Server (for Student and Personnel services) and Transporter.
- d. Third party applications or OS options may also perform network functions. These include byRequest and fairly standard printing protocols (Printer, NetPrint, and JetDirect). Additions to this list will be reviewed and will initially be treated as exceptions.
- e. Web-based system management tools will not be used. Exceptions can be made if:
 - i. The HP Web console is configured to the Bellevue College standard.
 - ii. The management tool has secure user level authentication and can only be used on or within a secure network (not across the Internet). The use of SSL is highly recommended.
- f. FTP service will not be allowed, as it completely bypasses the computer's security system. Note: This is in reference to FTP acting as a server or listening process accepting login requests, not FTP running as a client connecting from the HP3000 computer to a remote host.
- g. All other network services (i.e., inbound to the HP3000) will be treated as an exception and must be documented as defined above.

2. Dial-in Access and Modems

- a. Limited modem access will be supported to enable remote support, principally after hours.
- b. Logins originating from a modem will require an additional terminal password. This password will be defined and managed in accordance with the Bellevue College IT security standard addressing "Password Management."

3. Backups and System Recovery

- a. System recovery media will be created and kept current by authorized personnel so the system can be recovered to a known good state in the event of a system failure or compromise.
- b. System recovery documentation, outlining how to recover a system "from bare metal" will be available on paper or digital media.
- c. The recovery media and documentation will be stored in a location providing restricted access control, known to all systems administration staff, and will be reasonably accessible in the event it is required.
- d. Backup cycle is:
 - i. Full backups five nights a week by SBCTC-IT authorized personnel.
 - ii. Partial backup one weekend day by Bellevue College IR authorized personnel.
- e. Restoring files from tape is an operation that will only be approved and performed by authorized IT support personnel or an authorized designee.

- f. Tape backup media will be kept in a daily/weekly/monthly/yearly rotation. A two-week period of daily backups is kept at an offsite data storage facility – rotated via three storage containers (two always offsite) and daily delivery service. Weekly, monthly and yearly tape backups will be archived at a contracted authorized offsite data storage facility.

4. Boot and Single User Mode

- a. As Bellevue College's MPE server is located in a restricted access computer facility, the use of ROM and single user mode passwords will not be required.
- b. Remote console (i.e., over a modem link via the systems access port) will be disabled.
- c. In the event of an unexpected reboot, the computer will be configured to complete the boot process without intervention. A short pause will be configured to allow an administrator to interrupt the boot process if needed -- 15 seconds is normally adequate for this pause.

5. File, Group, and Account Security

- a. Accounts with elevated privileges -- System Manager (SM), Privileged Mode (PM), Network Administrator (NA), Node Manager (NM) -- will have their access restricted to only members of the MPE systems administration group. (For more information, see the "*Elevated Privileges*" section of this document).
- b. Groups with elevated privileges – Account Manager (AM), System Supervisor (OP) – will be restricted to user's accounts where those privileges are appropriate, such as the manager of the account and the system operator. (For more information, see the "*Elevated Privileges*" section of this document).
- c. Files, especially databases, will not be released across accounts. The Systems Administrator, with an explanation of why it is necessary, will document any file that needs released in this manner.
- d. No account or group granted PM capability will have unrestricted save access (e.g., SAVE:ANY).
- e. The business application software, as well as the system software, will be protected from users on the computer system. This means they will not have the ability to write to or to delete the software.
- f. When an MPE user, group, or account is created, the default security assigned by the operating system will be reviewed for appropriateness.

6. Account Management

- a. All users will have their own user accounts; account sharing is not be allowed.
- b. MPE Session Name, User, and Account will be the required components defining an MPE user login account in the Washington Community and Technical College (WCTC) environment.
- c. All accounts will have Security3000 passwords. In addition, all accounts with SM capability will also have MPE user passwords.
- d. Accounts are granted for specific business need; when that need no longer exists, the account will be deleted.
- e. Account access will be controlled by password authentication in accordance with the Bellevue College IT security standard addressing "*Password Management.*"
- f. No more than five consecutive incorrect login attempts (password attempts) will lock an account. A systems administrator will be the only one who can unlock it. Appropriate warning banners will be displayed at login, as required by the the Bellevue College IT security standard addressing "*Login Banners.*"

- g. Inactive accounts (those that have not been logged into within the last ninety days) will be deactivated. If an account persists in an inactive state, the systems administrator will attempt to determine if it can be deleted.
- h. Idle terminal sessions that have not set a terminal lock will be logged off after 30 minutes of inactivity. If the session is for a user account with SM capabilities, the idle time will be shortened to 15 minutes.

D. General Management

1. Elevated Privileges

- a. System administration privileges (and responsibilities) will be granted only to the MPE systems administration group within Information Resources and, on occasion, to other trained staff in IR. The system administration privileges are defined as those user accounts that have been assigned the SM or PM capabilities. The user account SECURITY.SYS is an exception to this, as SM is required on the account to perform its function; but users will be captured within a restricted menu, limiting their available commands and actions.
- b. Other system capabilities that will be tightly controlled are: OP, NA, NM, and AM. These privileges will be granted to non-MPE systems administration. Historically, and with cause, applications support staff have been granted access to the MGR.Pnnn accounts, which have both AM and OP capabilities; and the CISuser CONSULT.Pnnn account will have OP capability. This access is necessary for support staff to perform job functions.
- c. Backdoor programs, whether third party or home-grown, which would allow users to elevate their ability to acquire SM, PM, NA, or NM privileges will not be used or will be disabled.
- d. Upon separation from Bellevue College, an IT support employee with management privileges will have all privileged access to the MPE server immediately revoked and passwords will be changed.

2. System Monitoring

- a. The SBCTC-IT Operations staff will remotely perform nightly monitoring of all Bellevue College's processors. The SBCTC-IT Operations staff will address any problems or the appropriate IR staff will be contacted.

3. Logging and Log Review

- a. The Security 3000 violations report will be reviewed on a daily basis by authorized IR IT support personnel.
- b. The Security 3000 maintenance report will be reviewed on a daily basis by authorized IR IT support personnel to assure all changes were correct and appropriate.
- c. System logging will be enabled for at least the following events:
 - i. Interactive and batch logins and logouts.
 - ii. Password changes.
 - iii. System startup, shutdown, and power failure.
 - iv. System logging configuration and management.
 - v. Hardware diagnostic messages.
- d. Security issues will be reported to the Bellevue College IT Security Administrator and or designee.

4. System Scan/Assessment

- a. These systems will receive periodic (no less than once a quarter) network vulnerability scans. Within the limitations of business need, all vulnerabilities

identified will be quickly rectified. Standard tools to perform these types of assessments include Nessus or Saint.

- b. Host-based system scans will be performed no less than once a year to review the host's internal security. Within the limitations of business need, all vulnerabilities identified will be quickly rectified. Standard tools to perform these types of assessments include Audit3000.
- c. The file systems will be scanned to assure no unnecessary files, groups, or accounts have SM or PM privilege, or are world-writable.
- d. Assessment reports will be forwarded to the Bellevue College IT Security Administrator to be reviewed and filed.

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. HP MPE Systems manuals that might be helpful include:
 - a. MPE XL General User's Reference Manual
 - b. System Startup, Configuration, and Shutdown Reference
 - c. Controlling System Activities
 - d. Performing System Manager Tasks
 - e. Performing System Operator Tasks
 - f. Glossary of Terms and Acronyms
1. SBCTC-IT IT Security Standard – MPE System Configuration
2. Bellevue College IT Security Policy
3. Bellevue College IT Security Standard: Password Management
4. Bellevue College IT Security Standard: Login Banners
5. Acceptable Use of the Bellevue College Network and Bellevue College Data Management Policy

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

Appendix B – Related Acronyms

MPE	MultiProcessing Executive—MPE consists of programs that handle exchanges between HP terminals, printers, storage devices, memory and executing programs.
NA	Network Administrator Capability—The user, selected by the system manager, who is assigned to manage the data communications subsystem at a specific location.
NFT	Network File Transfer—A network services (NS) user service that allows you to copy files from one node to another interactively or programmatically.
NM	Node Manager Capability—A capability assigned to users allowing them to control communication subsystems at their node.
NMMGR	Network Node Manager—Application that manages communication control to the nodes.
NODE	One end of a communication link or a computer system in a network.
NSIR	Network System Information Request
OP	System Supervisor Capability—Capability assigned by the system manager to the system supervisor's username and account. The system supervisor is responsible for performing backups, altering the system configuration.
OS	Operating System
PM	Privileged Mode Capability—Capability assigned to accounts, groups, or users allowing unrestricted memory access, access to privileged CPU instructions, and the ability to call privileged procedures.
RFA	Remote File Access Capability
RPM	Remote Process Management
SM	System Manager Capability—Capability that allows execution of all commands necessary to manage the system.
SNMP	Simple Network Management Protocol—a protocol that is used to manage TCP/IP networks
UDC	User Defined Commands
VT	Virtual Terminal—Service that provides interactive access to the desktop.
WCTC	Washington Community and Technical Colleges