

Server Security Standard

Revision Date:

1. Purpose: The purpose of this standard is to establish standards for the base configuration of internal server equipment that is owned and/or operated by any El Paso Community College (EPCC) department. Effective implementation of this standard will minimize unauthorized access to proprietary information and technology.

2. Scope: This standard applies to server equipment owned and/or operated by any EPCC department and to servers registered under any EPCC-owned internal network domain. This standard is specifically for equipment on the internal EPCC networks.

3. Description

Ownership and Responsibilities: All internal servers deployed at EPCC must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by the operational group, based on business needs and approved by security administration. This operational group will monitor configuration compliance and implement an exception policy tailored to their environment. The Chief Information Officer is the approving authority for each exception. The operational group must establish a process for changing the configuration guides, which includes review and approval by Information Security and senior Information Technology administration.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - Server contact(s) and location and a backup contact
 - Hardware and operating system/version
 - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration Guidelines

- Operating system configuration should be in accordance with approved guidelines for optimized hardening.
- The network will be compartmentalized into separate domains based on business function.
- Use Group Policy to ensure all network-attached computers remain in a secure configuration after they are deployed.
- System Administrators should use operating system vendor-specific security checklists for:
 - Domain controllers

- o IAS servers
- o Exchange servers
- o SQL servers
- o IIS servers
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods, such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- Administrators should have their own privileged account with the appropriate level of authority (up to an equivalent of root where appropriate). Administrators should only use their privileged account when necessary and use their 'regular' account in all other cases.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels (e.g., encrypted network connections using IPSec).
- The NTFS file system will be used exclusively.
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled areas.
- Every security template must be tested in a laboratory environment prior to deployment for production.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - o All security related logs will be kept online for a minimum of one week.
 - o Daily incremental tape backups containing security related logs will be retained for at least one month.
 - o Weekly full tape backups of logs will be retained for at least one month.
 - o Monthly full backups will be retained for a minimum of two years.
- Security-related events will be reported to the Chief Information Officer for internal audit. Logs will be reviewed and incidents reported to Information Technology management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - o Port-scan attacks
 - o Evidence of unauthorized access to privileged accounts
 - o Anomalous occurrences that are not related to specific applications on the host

Compliance

- Audits will be performed on a regular basis by authorized organizations within EPCC.

- The internal audit group, in accordance with the *Audit Standard*, will manage audits. Internal audit will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4. Enforcement: Violation of this standard may result in disciplinary action in accordance with El Paso Community College policy and procedures. If you need clarification of this standard, call the Information Security Manager at 831-6312 or make contact via e-mail or the IT Help Desk. The Information Security Manager may also be reached via the Office of the Chief Information Officer.