Server Security Policy

1.0 Purpose

Servers are critical components of the organization's IT infrastructure, hosting vital applications and sensitive data. Unsecured or improperly configured servers represent a significant vulnerability and a primary target for malicious actors. The purpose of this policy is to establish the minimum standards for the secure configuration, management, operation, and monitoring of all server equipment owned or operated by the organization on its internal networks. Adherence to these standards is crucial to minimize security risks, prevent unauthorized access, and protect the confidentiality, integrity, and availability of organizational information and technology assets.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel responsible for the deployment, administration, operation, or management of server equipment on the organization's internal network. It covers all physical and virtual servers owned, operated, or leased by the organization or registered under an organization-owned internal network domain. This policy applies specifically to internal servers; servers located in a Demilitarized Zone (DMZ) are subject to additional requirements outlined in the DMZ Equipment Policy.

3.0 Policy Statements

3.1 Ownership, Responsibility, and Registration

* **Ownership:** All internal servers must have a clearly designated owning operational group or department responsible for system administration and policy compliance.
* **Configuration Guides:** Each operational group must establish, maintain, and follow approved server configuration guides (secure baseline builds) tailored to their specific server roles and operating systems. These guides must be based on organizational standards and security best practices and require initial and ongoing review and approval by the designated IT authority (e.g., Precision Computer). A process for managing changes to these guides, including review and approval, must be in place.
* **Registration:** All servers must be registered in the organization's central asset management or enterprise management system. Registration information must be kept accurate and up-to-date, including at a minimum:
    * Server hostname and IP address(es).
    * Primary and backup administrator/owner points of contact (including location).
    * Hardware details and Operating System/Version.
    * Primary functions and applications hosted.
* **Change Management:** All configuration changes applied to production servers must follow formal organizational change management procedures.

3.2 Secure Configuration Requirements

*   **Baseline Conformance:** Servers must be configured in accordance with the approved secure configuration guides/baselines relevant to their operating system and function.
*   **Service Hardening:** Unnecessary services, applications, and network ports must be disabled or removed to minimize the server's attack surface.
*   **Patch Management:** Servers must be kept up-to-date with the latest security patches and updates provided by the OS and application vendors. Patches must be applied promptly according to the organization's vulnerability management timeline requirements, with documented exceptions only permitted for specific, approved business reasons requiring compensating controls.
*   **Principle of Least Privilege:**
    *   Services and applications should run under accounts with the minimum privileges necessary for their function. Use of highly privileged accounts (e.g., root, Administrator) should be restricted to essential administrative tasks.
    *   User access must adhere to the principle of least privilege, granting only the permissions required for assigned job duties.
*   **Trust Relationships:** System-level trust relationships (e.g., domain trusts, Kerberos delegation, SSH key-based trusts) must be implemented judiciously, documented, regularly reviewed, and avoided where alternative secure communication methods suffice.
*   **Secure Administrative Access:** Privileged access (administrative login) must be performed over secure, encrypted channels (e.g., SSH, TLS-protected protocols, console access via secure terminal servers). Unencrypted administrative protocols (e.g., Telnet, FTP) are prohibited.
*   **Access Control Logging:** Access to critical services should be logged and potentially protected by additional access control layers (e.g., web application firewalls for web services) where feasible.

3.3 Physical Security

*   Servers must be physically located within secure, access-controlled environments (e.g., data centers, locked server rooms) compliant with the organization's Physical Security Policy.
*   Operating servers from uncontrolled areas, such as user cubicles or open offices, is strictly prohibited.

3.4 Monitoring and Logging

*   **Audit Logging:** Servers must generate audit logs for security-relevant events as defined in the Audit Logging Policy. This includes logins (success/failure), privilege changes, configuration modifications, critical service start/stop events, significant errors, and security tool alerts.
*   **Log Forwarding:** Security-related logs must be forwarded to the organization's central logging system (SIEM) in near real-time.
*   **Log Retention:** Audit logs must be retained according to the following minimum schedule (or as defined by the organizational Record Retention Schedule, whichever is longer):
    *   Online (e.g., within SIEM): Minimum 1 week
    *   Offline Backups (e.g., daily incrementals): Minimum 1 month
    *   Offline Backups (e.g., weekly fulls): Minimum 1 month
    *   Offline Backups (e.g., monthly fulls): Minimum 2 years

*   **Log Review and Reporting:** Security-related events identified in logs or by monitoring systems (e.g., port scans, unauthorized privilege access attempts, anomalous system behavior) must be reported to and reviewed by the designated security authority (e.g., Precision Computer, Security Operations Center). This authority will coordinate incident response and prescribe corrective measures as needed.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including configuration audits against approved baselines, vulnerability scanning, penetration testing, review of change management records, physical security checks, log reviews, internal/external audits, and assessment of monitoring procedures.

4.2 Exceptions

Any exception to this policy requires formal, documented justification outlining the technical necessity or constraint, risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security). Operational groups managing servers should maintain a record of approved exceptions relevant to their systems.

4.3 Enforcement

*   Servers found to be non-compliant with this policy must be remediated within a defined timeframe or risk being isolated or removed from the network.
*   Failure by personnel responsible for server administration or management to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Server:** A computer system (physical or virtual) providing shared resources, services, or applications to other computers (clients) over a network.
*   **Baseline (Secure Configuration Guide):** A documented standard configuration defining the required security settings and software state for a specific operating system or server role.
*   **DMZ (Demilitarized Zone):** A perimeter network segment logically placed between an internal network and an external network (like the Internet).
*   **Least Privilege:** The security principle of granting users and processes only the minimum permissions necessary to perform their required functions.
*   **Trust Relationship:** A configured link between systems or domains allowing one system/domain to accept authentication or authorization decisions made by the other.

6.0 Related Policies

*   Audit Logging Policy
*   Change Management Policy

* Data Classification Policy
* DMZ Equipment Policy
* Information Security Policy (Overall)
* Password Policy
* Physical Security Policy
* Vulnerability Management Policy / Patch Management Policy
* Record Retention Schedule / Policy

Revision #2
Created 28 August 2024 16:58:16 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery