

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by People. Effective implementation of this policy will minimize unauthorized access to People proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at People and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by People or registered under a People-owned internal network domain.

4. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at People must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by People. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by People.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved People guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4 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.

4.2.5 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 is sufficient.

4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7 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 SSH or IPSec).

- 4.2.8 Servers should be physically located in an access-controlled environment.
- 4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2 Security-related events will be reported to the People Security Team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

5. Policy Compliance

5.1 Compliance Measurement

The People Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the People Security Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of Change	Responsible	Summary of Change
August 2014	Sat Sindhar	Introduced policy