**Server Security Policy**

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to* [*policy-resources@sans.org*](mailto:policy-resources@sans.org)*.*

**Last Update Status:** *Updated June 2014*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Valid from | Next Review | Authorised by | Date |
| 1.5 | 01/08/2022 | 01/03/2055 | Tagh Murray, Cybersecurity Team Lead | 23/05/2022 |

# 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.

to the window server estate. For other operating systems and IT infrastructure, they are here goes something else their own rules and refer to their own standards

New content

# 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 Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

# Scope

All employees, contractors, consultants, temporary and other workers at <Company Name> and its subsidiaries must adhere to this policy irrespective of where they are located. This policy applies to server equipment that is owned, operated, or leased by <Company Name> or registered under a <Company Name>-owned internal network domain.

Exempt from this are servers and other compute equipment that is operated in the cloud with the exception of SaaS cloud services which must strictly adhere to this policy.

# Policy

* 1. General Requirements
     1. All internal servers deployed at <Company Name> 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 InfoSec. 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 InfoSec. The following items must be met:
* 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
  + IP network identify and VPN token
  + 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
  + 1. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.
  1. Configuration Requirements
     1. Operating System configuration should be in accordance with approved InfoSec benchmark and standards.
     2. Services and applications that will not be used must be disabled where practical.
     3. Access to services have to be logged and/or protected through access-control methods such as a web application firewall, if possible.
     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.
     5. Trust relationships between systems are a security risk, and their use has to be avoided. Do not use a trust relationship when some other method of communication is sufficient.
     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.
     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).
     8. Servers must be physically located in an access-controlled environments.
     9. Servers are specifically prohibited from operating from uncontrolled cubicle areas.
  2. Monitoring
     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.
  + 1. Security-related events will be reported to InfoSec, 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.

# Policy Compliance

* 1. Compliance

The Infosec team has to determine compliance criteria for this policy. They may change from time to time as circumstance change. Following change, the Infosec team will advertise them on the social media channel of the <Company Name>.

* 1. Compliance Measurement

The Infosec 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.

# Exceptions

Any exception to the policy must be notified to the Infosec team in advance.

# Non-Compliance

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

# Related Standards, Policies and Processes

* Audit Policy
* Window OS Secure Baselines
* Linux OS Security Baselines
* CIS Benchmarks

# Definitions and Terms

List of definition and terms, and their respective meaning

* Authorized user – user that has unlimited access to network of <Company Name>
* VPN – virtual private network, secure connection from outside network of <Company Name>
* SSH – secure shell protocol used in Mac devices to connect to IT applications
* IPSec – IP Security team in charge of network security
* InfoSec – Information Security team in charge of data security

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| June 2022 | InfoSec | Updated and converted to new format. |
|  |  |  |