Server Audit 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.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to ensure all servers deployed at <Company Name> are configured according to the <Company Name> security policies. Servers deployed at <Company Name> shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Ensure conformance to <Company Name> security policies

3. Scope

This policy covers all servers owned or operated by <Company Name>. This policy also covers any server present on <Company Name> premises, but which may not be owned or operated by <Company Name>.

4. Policy

<Company Name> hereby provides its consent to allow <Internal or External Audit Name> to access its servers to the extent necessary to allow <Audit organization> to perform scheduled and ad hoc audits of all servers at <Company Name>.

4.1 Specific Concerns

Servers in use for <Company Name> support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

4.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

- All system logs shall be sent to a central log review system

- All Sudo / Administrator actions must be logged
- Use a central patch deployment system
- Host security agent such as antivirus shall be installed and updated
- Network scan to verify only required network ports and network shares are in use
- Verify administrative group membership
- Conduct baselines when systems are deployed and upon significant system changes
- Changes to configuration template shall be coordinated with approval of change control board

4.3 Responsibility
<Internal or External Audit Name> shall conduct audits of all servers owned or operated by <Company Name>. Server and application owners are encouraged to also perform this work as needed.

4.4 Relevant Findings
All relevant findings discovered as a result of the audit shall be listed in the <Company Name> tracking system to ensure prompt resolution or appropriate mitigating controls.

4.5 Ownership of Audit Report.
All results and findings generated by the <Internal or External Audit Name> Team must be provided to appropriate <Company Name> management within one week of project completion. This report will become the property of <Company Name> and be considered company confidential.

5. Policy Compliance

5.1 Compliance Measurement
<Internal or External Audit Name> shall never use access required to perform server audits for any other purpose
The Infosec Team will verify compliance to this policy through various methods, including but not limited to, 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 Infosec 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 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted format and retired.