SecOps® Solution

Server audit policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

A server audit policy ensures the security, integrity, and availability of sensitive information stored on a server. It helps detect and prevent unauthorized access and potential security breaches provide a record of system activity for auditing and compliance purposes and supports incident response and forensics activities.

2. Purpose

This policy's objective is to guarantee that all servers installed at **<Company Name>** are configured in accordance with **<Company Name>** security rules. Servers installed at **<Company Name>** must undergo audits at least once a year and in accordance with any necessary regulatory compliance.

3. Scope

This policy applies to all servers that **<Company Name>** owns or manages. This policy also applies to any servers that may be present on **<Company Name>** property but are not necessarily **<Company Name>** owned or managed.

4. Policy

By giving this consent, **<Company Name>** grants **<Internal or External Audit Name>** access to its servers to the degree required to enable **<Audit organization>** to conduct routine and emergency 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 an 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 the 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: The Infosec team must beforehand approve any exception to the policy.

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. Definition and Terms

None

8. Revision History

Version	Date	Description
1.0	07-02-2023	Initial Policy