CloudServe System Monitoring and Logging Policy

Effective Date: 9/9/2024
Last Updated: 9/9/2024
Version: 1.0

---

1. Purpose

The purpose of this System Monitoring and Logging Policy is to define the procedures for monitoring, logging, and reviewing activities on CloudServe's systems and infrastructure. This ensures timely detection of security incidents, operational issues, and compliance with the SOC 2 Trust Service Criteria for Security, Availability, and Confidentiality.

---

2. Scope

This policy applies to all CloudServe systems, networks, databases, and applications that store or process customer, employee, or internal business data. It covers activities performed by CloudServe employees, contractors, and third-party vendors.

---

3. Monitoring Objectives

The primary objectives of monitoring and logging include:

- Detecting unauthorized access, system anomalies, or malicious activity.
- Monitoring system performance and availability.
- Logging changes to critical systems, including access control, system configurations, and user activities.
- Ensuring compliance with regulatory requirements and internal policies.
- Supporting incident response efforts and forensic investigations.

---

4. Logging Standards

Logs must be generated and maintained for the following key events:

- **User Authentication and Access**: Login attempts (both successful and failed), logouts, password changes, and privilege escalation.

- **System Changes**: Modifications to system configurations, software updates, and installation of new software or hardware.
- **File and Data Access**: Access to sensitive or confidential data, including attempts to view, modify, delete, or transfer data.
- **Security Incidents**: Detection of malware, unauthorized access, DDoS attacks, or any suspicious activities.
- **Network Activity**: Monitoring of inbound and outbound traffic, network connection attempts, and abnormal traffic patterns.

Logs should include relevant metadata such as:

- **Timestamp** (with time zone information)
- **User or System ID**
- **IP Address**
- **Event Description**

---

5. Log Retention and Storage

- **Retention Period**: Logs must be retained for at least 12 months to allow for audits, incident investigations, and system analysis. Extended retention may be required based on legal or contractual requirements.
- **Storage**: Logs must be stored in a secure, centralized logging system with redundancy measures in place. Access to logs should be restricted to authorized personnel only, and logs must be encrypted both in transit and at rest.
- **Backup**: Logs should be backed up regularly (e.g., daily or weekly) and stored securely, separate from production systems.

---

6. Monitoring Systems

CloudServe will employ the following tools and techniques to ensure continuous monitoring:

- **Intrusion Detection and Prevention Systems (IDPS)**: Monitors network traffic for malicious activity and potential threats.
- **Security Information and Event Management (SIEM)**: Aggregates log data from multiple systems and analyzes it for patterns that may indicate security breaches.
- **Performance Monitoring Tools**: Tracks system uptime, resource usage, and performance metrics to ensure systems remain available and operational.
- **Automated Alerts**: Generates alerts for suspicious or unauthorized activities, system failures, or performance degradation.

---

7. Review and Analysis

- **Daily Monitoring**: System logs and security alerts must be reviewed daily by the IT and Security teams to detect any abnormalities or threats.
- **Regular Audits**: Logs must be audited at least quarterly to identify trends, potential vulnerabilities, and areas of improvement.
- **Incident Review**: In the event of a security breach or incident, logs must be analyzed immediately to determine the cause and extent of the breach and to support the incident response process.

---

8. Roles and Responsibilities

- **IT Department**: Responsible for maintaining the logging systems, ensuring logs are collected, and investigating system performance issues.
- **Security Team**: Responsible for monitoring security-related events, analyzing logs for threats, and responding to incidents.
- **Compliance Team**: Ensures that log retention policies comply with SOC 2 requirements, as well as any applicable legal or contractual obligations.
- **Data Owners**: Responsible for ensuring that systems storing sensitive data are monitored and that access to logs is restricted to authorized personnel.

---

9. Security and Access Controls

- **Access Control**: Only authorized personnel should have access to logs. A role-based access control (RBAC) model must be applied to ensure only the necessary individuals can view or modify logs.
- **Log Integrity**: Logs must be protected from unauthorized alteration. Measures such as digital signatures or hashing should be used to ensure log integrity.
- **Encryption**: All logs must be encrypted during transmission and while at rest to prevent unauthorized access.

---

10. Policy Compliance and Violations

Compliance with this policy will be regularly monitored, and audits will be conducted to ensure its effectiveness. Any failure to adhere to this policy may result in disciplinary action, up to and including termination of employment or vendor contracts.

---

11. Review and Updates

This policy must be reviewed and updated at least annually or whenever there is a significant change to CloudServe’s systems, infrastructure, or legal requirements.

---

12. Contact Information

For questions or concerns about this policy, please contact the IT or Security Team at CloudserverIT@CS.com.