Audit Log Policy and Procedure

1. Purpose

The purpose of this policy is to establish guidelines for the collection, review, and retention of audit logs to ensure the integrity, availability, and confidentiality of log data. Audit logs are crucial for monitoring and identifying unauthorized or anomalous activities, supporting forensic investigations, and complying with legal and regulatory requirements.

2. Scope

This policy applies to all systems, devices, and applications that generate audit logs within the organization. It covers all departments, employees, and contractors who interact with or manage these systems.

3. Policy Statement

The organization commits to maintaining a comprehensive audit log management system that captures, reviews, and retains log data in a secure and efficient manner.

4. Responsibilities

- **IT Security Team**: Responsible for the overall management of the audit log process, including collection, review, and retention of logs.
- **System Administrators**: Accountable for configuring and maintaining log generation and collection in accordance with the policy.
- **Audit Team**: Tasked with regularly reviewing audit logs to identify and investigate suspicious activities.

5. Procedures

5.1 Audit Log Collection

- Ensure that all critical systems, devices, and applications are configured to generate comprehensive audit logs.

- Implement centralized log management solutions to collect and store logs securely.
- Protect log integrity by implementing controls to prevent unauthorized modification or deletion.

5.2 Audit Log Review

- Conduct regular reviews of audit logs to identify any indications of suspicious, unauthorized, or anomalous activities.
- Utilize automated tools for continuous monitoring and alerting on potential security incidents.
- Document the review process, findings, and any actions taken in response to detected incidents.

5.3 Audit Log Retention

- Retain audit logs for a period consistent with legal, regulatory, and organizational requirements.
- Store logs securely to prevent unauthorized access, modification, or destruction.
- Ensure that retained logs can be easily accessed and analyzed when needed.

6. Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract termination. Compliance will be monitored by the IT Security Team and reported to executive management.

7. Review and Revision

- Review and update this policy and its procedures annually or when significant changes to the systems or operations occur.
- Revisions should reflect changes in technology, threats, legal and regulatory requirements, and business operations.

By implementing this audit log policy and procedure, the organization can effectively monitor, detect, and respond to potential security incidents, ensuring the ongoing security and integrity of its information systems.