SOP: Audit Trail Creation and Monitoring

This SOP establishes the procedures for **audit trail creation and monitoring** to ensure accurate tracking of system activities, enhance security, and maintain accountability. It details the methods for generating comprehensive audit logs, monitoring user actions, detecting unauthorized access, and reviewing audit data regularly to support compliance and operational integrity.

1. Purpose

To define the process for creating, monitoring, and maintaining system audit trails that track user activities and events, ensuring compliance, data integrity, and security.

2. Scope

This SOP applies to all information systems and users within the organization that process, store, or transmit sensitive or regulated data.

3. Responsibilities

Role	Responsibilities
System Administrators	Set up and maintain audit logging; monitor and review audit logs; report suspicious activity.
IT Security Team	Perform periodic log analysis; respond to incidents; maintain security of audit trail systems.
Managers	Ensure compliance with SOP requirements within their departments.

4. Procedures

4.1 Audit Trail Creation

- Enable audit logging on all critical systems and applications.
- Configure logs to capture key activities:
    - User logins and logouts
    - Failed login attempts
    - File and data access/modifications
    - Administrative privilege use
    - System configuration changes
- Ensure logs capture date, time, user ID, event description, and source IP.

4.2 Audit Trail Monitoring

- Monitor audit logs daily for unusual or unauthorized activities.
- Set up automatic alerts for high-risk events (e.g., privilege escalation, multiple failed logins).
- Use log management tools to centralize and analyze audit data.

4.3 Detection of Unauthorized Access

- Review alerts and flagged activities promptly.
- Investigate and document incidents of unauthorized access following the organization's incident response plan.

4.4 Audit Trail Review

- Conduct periodic (at least monthly) reviews of audit logs.
- Document findings and corrective actions for any anomalies.
- Report audit review outcomes to management.

4.5 Log Retention and Protection

- Retain audit logs for a minimum period as defined by policy or regulations (e.g., 1 year).
- Protect logs from unauthorized access, alteration, or deletion.
- Back up logs regularly and store backups securely.

5. Compliance and References

- Comply with relevant standards (e.g., ISO 27001, HIPAA, GDPR).
- Refer to related organizational policies: Information Security Policy, Incident Response Policy.

6. Revision History

Version	Date	Description	Author
1.0	2024-06-17	Initial version	IT Security