SOP: Audit Trail and Activity Logging Requirements

This SOP defines **audit trail and activity logging requirements** to ensure accurate tracking of user actions, system changes, and data access within an organization. It includes guidelines for capturing, storing, and protecting logs to maintain data integrity, support compliance with regulatory standards, facilitate forensic analysis, and enhance security monitoring. The purpose is to provide a comprehensive record of activities that enables accountability and transparency, aiding in the detection and investigation of unauthorized or suspicious behavior.

1. Purpose

To establish requirements and procedures for audit trail and activity logging within the organization, supporting regulatory compliance, forensic investigation, and security monitoring.

2. Scope

This SOP applies to all information systems, applications, and users under the organization's control that process, store, or transmit sensitive or regulated data.

3. Responsibilities

- **System Administrators:** Ensure logging is enabled, logs are secured, and retention policies are enforced.
- **IT Security Team:** Monitor logs, investigate anomalies, and respond to incidents.
- **Data Owners:** Define requirements specific to their data and systems.
- **All Users:** Adhere to organizational policies related to their actions and system access.

4. Audit Trail and Logging Requirements

Requirement	Description
Events to Log	• User authentication (logins, logouts, failed attempts) • Privilege and role changes • Access to sensitive data • Configuration and system changes • Creation, deletion, and modification of user accounts • Use of administrative functions • File and data exports • System errors and exceptions
Log Contents	• Date and time of the event (with UTC timestamp) • User identity (username, user ID) • Source IP address or host • Event description and outcome
Log Retention	• Retain logs for at least 12 months, or as required by law or policy. • Periodically archive older logs securely.
Log Protection	• Restrict access to authorized personnel only. • Ensure logs cannot be modified or deleted by unauthorized users. • Utilize encryption for log storage and transmission.
Monitoring & Review	• Regularly review logs for suspicious or unauthorized activities. • Implement automated alerts for critical security events. • Document and follow up on all identified incidents.
Backup & Recovery	Include audit logs in regular backup processes and test recovery periodically.

5. Procedures

1. **Enable Logging:** Configure all relevant systems and applications to capture required audit events.
2. **Secure Log Storage:** Store logs in a secure location with appropriate access controls.
3. **Retention & Archiving:** Regularly archive logs in accordance with policy and automate retention enforcement where possible.
4. **Monitoring:** Continuously monitor logs for anomalies using automated tools and manual review.
5. **Incident Response:** Investigate any suspicious or unauthorized activities recorded in logs and take necessary actions.
6. **Review & Update:** Annually review logging configurations and this SOP to ensure compliance and relevance.

6. Compliance

All staff must comply with this SOP, relevant data protection regulations (e.g., GDPR, HIPAA), and applicable organizational policies.

7. References

- GDPR Article 30 (Records of processing activities)
- NIST SP 800-92 (Guide to Computer Security Log Management)
- HIPAA Â§164.312(b) (Audit Controls)
- ISO/IEC 27001:2013 A.12.4 (Logging and monitoring)

8. Revision History

Date	Version	Description	Author
2024-06-04	1.0	Initial SOP release	[Your Name]