Popular Vehicles
& Services

Policy Related to Information Technology Security

LOGGING, MONITORING & AUDIT TRAIL POLICY

Document Title : Logging, Monitoring & Audit Trail Policy

Version : 1.0

Effective Date : 31-01-2026

Review Cycle : Annual

Policy Owner : IT / Information Security

Approval Authority : Management / Board of Directors

1. Purpose

The purpose of this policy is to define requirements for logging, monitoring, and audit trails to ensure that system and user activities are properly recorded, retained, and reviewed. This policy supports security monitoring, incident investigation, operational troubleshooting, and Information Systems (IS) audit requirements.

2. Scope

This policy applies to all servers, systems, applications, and infrastructure, including Windows-based servers and endpoints, web servers and applications hosted on IIS, databases supporting business applications, and on-premises and cloud-hosted environments. It covers system, application, database, and security event logs.

3. Logging Principles

The organization shall:

- Enable logging on critical systems, applications, and databases

- Ensure logs are protected against unauthorized access, modification, or deletion

- Retain logs for a defined period based on audit, regulatory, and business requirements

- Review logs to identify security incidents, operational issues, and compliance risks

4. Types of Logs Covered

4.1 Windows Event Logs

The following Windows Event Logs shall be enabled and maintained:

- Application Logs – application errors, warnings, and informational events

- System Logs – operating system, service, and hardware-related events

- Security Logs – authentication, authorization, and security-related activities

4.2 IIS Logs

IIS logging shall be enabled for all web applications and shall capture:

- HTTP requests and responses

- Status codes (e.g., 200, 404, 500)

- Client IP addresses, URLs accessed, and timestamps

4.3 Security Logs

Security logs shall record:

- User logon and logoff activities

- Privileged and administrative actions

- Security configuration and policy changes

4.4 Database Logs

Database logging shall be enabled for all critical databases to record:

- Database authentication and access activities

- Administrative and privileged database actions

- Significant database system events

Database logs shall be protected against unauthorized access or modification and retained to support security monitoring, incident investigation, and audit requirements.

---

5. Log Retention

- Logs shall be retained for a defined retention period based on system criticality, audit requirements, and storage capacity

- Security and database logs shall be retained for a longer duration due to their importance for investigations and audits

- Log retention configurations shall be reviewed periodically to ensure adequacy

6. Log Review and Monitoring

- Logs shall be reviewed periodically and when required, including during security incidents, system or application issues, and audit activities

- Log reviews shall focus on identifying unauthorized access attempts, errors, and suspicious or abnormal activities

7. Roles and Responsibilities

IT / Information Security:

- Enable and maintain logging configurations
- Ensure logs are securely stored and retained
- Perform or coordinate log reviews and investigations
- Maintain audit evidence related to logging and monitoring

Management / System Owners:

- Ensure logging requirements are implemented for systems under their responsibility
- Support remediation of issues identified through log reviews

8. Audit and Evidence

The following audit evidence shall be maintained and made available upon request:

- Configuration evidence showing logs are enabled (Windows, IIS, databases)
- Log retention settings
- Sample system, application, IIS, and database log files
- Records of log reviews, investigations, or incident handling

9. Compliance

Compliance with this policy is mandatory. Non-compliance may result in disciplinary action in accordance with organizational policies and applicable laws. Approved exceptions shall be formally documented.

10. Review

This policy shall be reviewed annually, or earlier in the event of significant changes to systems, logging mechanisms, or audit requirements.

11.Approval

This policy has been reviewed and approved by the following authorities:

Role	Name	Signature	Date
Board of Directors / management			
Head – IT			