Azure Monitoring & Audit Policy

Policy Number: IT-MA-004
Date Adopted: September 17, 2025
Last Revision: September 17, 2025
Last Review: September 17, 2025

1. Purpose
To establish requirements for monitoring, logging, and auditing Entra ID and Azure activity to ensure security, compliance, and accountability.

2. Applicability
This policy applies to:

- All employees, contractors, and third-party users accessing Entra ID or Azure resources.
- All Azure services and subscriptions where activity logging and monitoring are supported.

3. Accountability

- **IT / Security Team:** Responsible for configuring logs, monitoring activity, and conducting audits.
- **Managers:** Ensure team members comply with logging and monitoring requirements.
- **Users:** Must not interfere with monitoring or audit systems.

4. Definitions

- **Entra ID Sign-in Logs:** Logs of authentication events, including successful and failed sign-ins.
- **Audit Logs:** Records of changes to users, groups, roles, and policies in Entra ID.
- **Azure Activity Logs:** Record of all management events in Azure subscriptions.
- **Microsoft Sentinel:** Cloud-native SIEM for detecting and responding to threats.

5. Policy

- Enable Azure Activity Logs and Entra ID Sign-in and Audit Logs across all subscriptions; retain logs for at least 12 months.
- Configure Microsoft Sentinel to alert on suspicious activity, such as failed logins, privilege escalations, or policy changes.
- Review role assignments, configuration changes, and privilege elevations at least bi-weekly.

- Export and archive monitoring and audit reports securely for compliance and review purposes.
- Integrate monitoring and audit processes with incident response workflows for rapid remediation.

6. Non-Compliance and Sanctions

Violations may result in:

- Revocation or restriction of access privileges.
- Written warnings or other disciplinary action.
- Escalation to management or HR.
- Reporting to legal or regulatory authorities if required.