

Audit and Accountability Policy

Purpose

When something goes wrong, Your Organization needs to be able to answer what happened, when, and who or what caused it. This policy defines how Your Organization generates, protects, and reviews audit logs across its information systems so that security-relevant events are traceable to an individual or process, detectable in a timely manner, and preserved for investigation.

Scope

This policy applies to all Your Organization information systems that store, process, or transmit company or customer data, including applications, infrastructure, identity systems, network devices, and the logging and monitoring platforms that aggregate their output.

What is logged

At minimum, Your Organization systems log: authentication events (success and failure), authorization and privilege changes, access to Confidential or Restricted data, administrative and configuration changes, and security-relevant system events (service starts/stops, audit-logging failures). Each log entry captures, where technically feasible: timestamp, user or process identity, event type and outcome, and the affected resource — sufficient to establish individual accountability for the action taken.

Time synchronization

All systems that generate audit logs synchronize their clocks to an authoritative time source so that events across systems can be correlated accurately.

Log protection

- Audit logs are protected from unauthorized access, modification, and deletion. Write access to production log stores is restricted to the logging pipeline itself; read access is restricted to authorized security and operations personnel.
- Where feasible, logs are shipped to a centralized, access-controlled logging platform separate from the systems that generate them, so that a compromised system cannot be used to erase its own trail.
- Audit logging failures (log pipeline down, storage full) generate an alert to IT/Security Operations so gaps in coverage are identified promptly rather than discovered during an investigation.

Log review

- Security-relevant logs (authentication anomalies, privilege escalation, access to Restricted data, alerts from monitoring tooling) are reviewed on a defined cadence — continuously via automated correlation/alerting where tooling supports it, supplemented by periodic manual review.
- Review findings that indicate a possible security event are escalated per the Incident Response Plan.
- Log review activity itself (who reviewed, when, findings) is documented to support audit evidence.

Log aggregation and correlation

Where Your Organization's scale and risk profile warrant it, logs from multiple sources are aggregated into a SIEM or equivalent platform to support correlation across systems, reducing the time to detect multi-stage attacks that would not be visible from any single system's logs alone.

Retention

Audit logs are retained for a period consistent with the Data Retention Policy and applicable legal, regulatory, and contractual obligations, balancing storage cost against the operational and investigative value of historical log data.

Roles and responsibilities

- **IT and Security Operations.** Owns logging infrastructure, log review cadence, and alert triage.
- **Engineering.** Ensures applications emit sufficient audit-relevant events and honors logging standards during development.
- **Information Security.** Sets logging and retention standards, and audits logging coverage against this policy.

Review cadence

This policy is reviewed annually by Information Security and IT Operations, or sooner following a gap in log coverage discovered during an incident or audit.

Effective date: [the date this policy takes effect]