audit-logs-collection-review-policy.md

# Audit Logs Collection & Review Policy

Purpose

This policy describes how admin and application audit logs are collected, retained and reviewed for systems that store Platform Data. Reviews are performed at least once every 7 days.

Scope

This applies to all backend services and admin consoles that access or store Platform Data for the AutoPromote application.

What we log (minimum required)

- Unsuccessful and successful admin login attempts
- Creation, modification, and deletion of admin accounts and roles
- Granting/revoking of admin privileges to accounts
- Creation, modification, and deletion of production data affecting user records
- Changes to authentication/configuration that affect access controls

Collection & Storage

- Audit logs are captured by the service responsible for each component (Express API, Firebase/Firestore admin actions, cloud provider audit logs). Logs are aggregated into a centralized logs store (e.g., Cloud Logging, ELK, or other SIEM).
- Each log entry contains a UTC timestamp, source service, event type, redacted identifiers, and an actor (role or admin id) when available.

Retention

- Audit logs are retained for a minimum of 90 days (or longer if required by regulatory needs). Older logs are archived according to the retention policy.

Review frequency & process

- Logs are reviewed at least once every 7 days by the security operations owner. Reviews include:
  - Automated alerts for suspicious events (failed login bursts, privilege escalations, deletion of audit logs)
  - Manual review of aggregated event summaries and exceptions
  - Generating an incident/ticket when suspicious activity is confirmed

Automated monitoring & evidence

- We run automated scans/alerts that monitor logs and create alerts or tickets in our tracking system (example acceptable evidence: screenshot of alert in Slack, a Jira ticket created by the monitoring tool, or CLI output showing flagged events).

Escalation

- If a review identifies a confirmed security-relevant event, escalate to the security lead and create an incident in the incident tracking system (include timeline, affected systems, and mitigation steps).

Responsibilities

- Security Owner: performs weekly reviews and signs off
- DevOps/Engineering: ensures logging is enabled and logs are shipped to the aggregator
- Application Owners: investigate and remediate issues raised from audit reviews

How to produce evidence for Facebook review

1. Provide this policy document and highlight the sections that state a weekly review cadence, the events logged, and escalation steps.
2. Provide a recent (within 3 months) output showing logs are collected with timestamps and event types. This can be:
   - A dashboard screenshot (redact PII) showing admin audit logs and dates, or
   - A directory listing of archived log files with timestamps, or
   - A text/CSV file (redacted) showing event type and timestamp.
3. Provide evidence of automated monitoring: a screenshot of an alert, a Slack/Jira ticket, or CLI output that shows an alert was generated by our monitoring tool.

Redaction guidance

- Remove or redact user-identifiable information and secrets before uploading.

Contact

- Security Owner: security@example.com