Final Frame™

Logging and monitoring policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	Application logs, cloud audit logs, the product audit trail, alerting
Review	27 October 2027
MPA CSBP	TS-1.5, TS-8.0, OP-3.0, OR-4.0

Approved by Robin Ashford, Founder, 27 October 2026

Three records, three jobs

Record	What it is	Kept
Product audit trail	Who did what to an Org's work: uploads, receipts, removals, deliveries, every download, view and preview link issued, sign-ins, status changes, memberships, roles, invitations, impersonation, settings, and the Screening Room's CMS acts and Analytics reads	Life of the Org
Cloud audit logs	Changes to Google Cloud configuration and IAM (Admin Activity). Data Access logs for Cloud KMS, Secret Manager and Cloud Storage	Admin Activity 400 days, locked. Data Access 365 days, locked

CSBP TS-1.5 and OP-3.0 ask for one year of logs.

Never logged

Secrets, passwords, session cookies, tokens, API keys, signed URLs, full request bodies, media contents. A failed sign-in logs the email address and nothing else about the attempt.

- A field with a sensitive name loses its value at any depth.
- A deliberate case carries // log-secrets-ok: <why>.
- A failed idle database connection logs one line with its message and code, never the client.

What must be logged

- Every request, with the fields above.
- Every sign-in success and failure, with method and IP, in the application logs and in the audit trail of each Org the person belongs to.
- Every download, view, proxy and preview link issued: actor, Org, object, expiry. Downloads from v1, MCP and the app's Download buttons write.
- Every platform-plane action, at warn level, including cross-Org reads and Org deletion.
- Every cloud configuration change (automatic, Admin Activity logs).

Background code writes JSON lines through, the same shape as the request logger, with wherever the work has an Org.

The Screening Room

What happens	What the record holds
A guest signs in, signs out or accepts the NDA	Guest, viewer session, IP address, user agent, request id
A member or a guest opens a title, starts a play, plays on (at most every 20 seconds of a play) or finishes	Member or guest, viewer session, play, title, position, duration, audio and subtitle language, IP address, user agent, request id
A member or a guest opens a search result	Member or guest, what was opened, the words that found it, IP address, user agent, request id
A guest is locked, held or unlocked	The failure count, the minutes, the actor for an unlock
A guest is invited, sent the invitation again, changed, put in viewer groups, revoked or reset	Actor, guest, before and after; the invitation rows carry the address and whether it was sent
Grants, viewer groups, collections and their audiences, scheduling, an acquired title included, rails, themes, the hero, settings	Actor, subject, before and after. Settings record the NDA text and the logo as set or not, never their content
Analytics read or exported	The view, the period, the filters, whether it named people or companies, the rows
A call the viewer host refuses	Route, method, origin and Sec-Fetch-Site where relevant

Never logged here: the address a link is asked for, a link or session token, a binding cookie, a passkey answer, an authenticator secret or code, a signed stream link. The door's log lines name a guest by id.

The guest door has its own alert (below) before the viewer host takes guests.

Alerts

Cloud Monitoring alert policies, sent to Robin by email and to his phone:

Alert	Condition
Service down	Uptime check on www or /readyz fails (checks every 60 s from six regions)
Not ready	The app not ready for 3 minutes; database auto-recovery acted or needs a person
Error rate	Server errors (5xx) above 5 in 5 minutes
Database	CPU above 80% for 5 minutes; connections failing or the model unreachable
Sign-in attack	More than 5 failed sign-ins in 10 minutes, or 429s at the load balancer
Impersonation	Any "View as" started
Platform admin	Any platform-admin session or action, and any platform-admin route refused
Key creation	A service account key or HMAC key made
IAM change	Any SetIamPolicy on the project, a bucket or a key
Bucket exposure	Any change to a bucket's IAM or public access prevention
Key change	Any KMS key version disabled, destroyed or scheduled for destruction
Secret access	A secret read by any identity other than the runtime service account
Backup failure	A Cloud SQL backup that did not complete
Worker stuck	No worker job completion for 30 minutes while jobs are queued

Alert	Condition
Jobs and spend	More than 40 job executions in an hour, more than 6 running at once, or model spend in a day above a set amount
Guest door	Link floods, lockouts and holds, and refused cross-site calls on the viewer host

Review

- Alerts: answered as they arrive. Each alert that turns out to be real becomes an incident.
- Weekly: Robin scans the error log for new error types, and the platform plane log.
- Quarterly: with the access review, read impersonation and platform admin activity for the quarter.
- Record each weekly and quarterly review with its date.

Protection of logs

- Only Robin can read logs. The runtime service account can write, not read or delete.
- Logs stay in Google Cloud and are read there.

Time

All services use Google's time source. Every log line and audit row is UTC.