

LagosPM Project Tracker

User and operations guide

A concise guide to signing in, maintaining project records, controlling costs and risks, administering access, and operating the Node.js and SQLite deployment safely.

Start with the Portfolio view for executive status. Use Projects for record-level work, and Admin for users and the immutable audit trail.

AREA	USE
Portfolio	Status, budget, forecast, risk, and recent activity overview.
Projects	Filter, open, register, and update delivery records.
Pipeline	Review projects grouped by development phase.
Costs	Compare approved budgets, commitments, actuals, and forecasts.
Risks	Prioritize exposure by probability × impact and track mitigation.
Admin	Manage users and review the dated audit history.

Prepared for the Ubuntu / Nginx / systemd deployment package · 04 September 2026

Sign in and choose the right role

First sign-in

- Enter the user ID or email address supplied by an Admin.
- Enter the temporary password. Repeated failed attempts are throttled.
- When prompted, replace it with a unique password of at least 12 characters containing upper case, lower case, a number, and a symbol.
- The application opens the Portfolio view after the password change succeeds.

Never share accounts or reuse the bootstrap Admin password. The temporary password must be delivered through an approved secure channel.

Roles

ROLE	CAN DO	CANNOT DO
Viewer	Read dashboards, projects, risks, costs, history; export CSV.	Create or change records; use Admin.
Editor	Viewer access plus create/update projects, development, costs, activity, and risks.	Manage users or read the Admin audit endpoint.
Admin	All Editor functions plus user access and audit review.	Bypass audit, CSRF, or password policy.

Find anything quickly

- Select the search pill in the top bar or press Ctrl+K.
- Type a view name, project code, or project name.
- Use the arrow keys and Enter to open the selected result; press Escape to close.

Keep the project record current

Register a project

- Open Projects and select Add project.
- Use a unique project code, choose a portfolio, and enter a descriptive name, phase, status, owner, approved budget, dates, and delivery description.
- Save. The project appears in the register and a dated creation entry is written automatically.

Work in the project dialog

TAB	WHAT TO MAINTAIN
Overview	Core status, phase, manager, dates, percent complete, budget, and description.
Development	Planning, design, procurement, construction, next gate, and the full narrative.
Costs	Dated entries for committed, actual, and forecast values.
Risks	Title, context, probability, impact, owner, mitigation, due date, and status.
History	Chronological updates and changes attributed to the signed-in user.

Safe concurrent editing

Every project has a version number. If another user saves first, your stale edit is rejected instead of silently replacing their work. Close and reopen the record, review the newer data, then apply your change again.

CSV export

Select Export CSV in Projects. The export includes codes, portfolio, delivery position, financial totals, dates, description, and last-updated time. It respects your authenticated session and safely quotes commas, line breaks, and quotation marks.

Costs, risks, and decisions

Cost control

- Approved budget is the authorization baseline on the project record.
- Committed, actual, and forecast totals are calculated from dated cost entries.
- Forecast variance is forecast minus approved budget. A positive value indicates forecast pressure.
- Never replace historical entries to hide a change; add the current dated position and explain it in project activity.

Risk control

- Probability and impact use a 1–5 scale. Exposure is their product.
- Name an accountable owner and write a concrete mitigation, not a status restatement.
- Use Open while action is required, Monitoring after the response is implemented, and Closed only when the exposure is no longer active.
- High exposures remain visible in the portfolio summary until closed.

A useful update answers four questions: what changed, why it matters, who owns the next action, and when the next decision is due.

Status language

STATUS	USE WHEN
On track	Delivery is within approved tolerances and no escalation is required.
Watch	A developing issue needs active monitoring but remains recoverable.
At risk	A material delivery, cost, scope, or approval outcome needs intervention.
On hold	Work is intentionally paused by an authorized decision.
Complete	Delivery and required closeout are finished.

Users, audit, and security

User lifecycle

- Admins create a user with display name, unique ID, email, and the minimum required role.
- The generated temporary password is displayed once. Deliver it securely; it cannot be recovered later.
- Use Reset password when access is lost. The new temporary password forces another change.
- Deactivate accounts promptly when access is no longer required. Do not recycle identities.

Audit trail

Admin shows dated authentication, project, risk, cost, and user-management events with the responsible account and network address. Audit entries are append-only through the application. Investigate unexpected access, bursts of failed sign-ins, privilege changes, and out-of-hours data changes.

Security model

- Passwords are salted and hashed; plaintext passwords are never stored.
- Session cookies are HttpOnly, SameSite=Strict, and Secure in production.
- State-changing requests require the session CSRF token and a matching origin.
- Authorization is checked by the server even when a control is hidden in the interface.
- The Node.js service listens only on localhost behind Nginx HTTPS.

If compromise is suspected: disable the account, preserve audit and Nginx logs, rotate credentials, verify the database and backups, and document the incident before restoring access.

Back up, restore, and release safely

Daily operations

- Monitor ``lagospm.service``, Nginx, disk space, certificate expiry, backup completion, and failed sign-ins.
- Back up with the supplied SQLite online-backup script; it validates the copy before compression.
- Copy encrypted backups off-host and perform a documented restore rehearsal.

Release flow

- Install each build into a timestamped immutable release directory.
- Run the automated tests before switching ``/opt/lagospm/current``.
- Verify localhost health, HTTPS sign-in, role boundaries, counts, writes, export, and audit.
- Keep the prior release and a matching pre-migration database backup until acceptance.

D1 migration gate

Import into a disposable SQLite target first. Reconcile source and target counts, run foreign-key and integrity checks, and inspect long narratives such as Parks and Resorts. Exact acceptance requires the stated 74 records on both sides; the original source export must be provided before this gate can close.

Support checklist

SYMPTOM	FIRST CHECK
Cannot sign in	User ID/email, active status, temporary-password change, throttling window.
Cannot edit	Role, session expiry, CSRF/origin, and whether the record version is stale.
Site unavailable	Nginx status, service status, localhost health, logs, disk space.
Data looks old	Selected filters, project history, importer counts, database path.
Restore needed	Backup integrity, maintenance window, matching release, post-restore checks.

Detailed commands and procedures are included in the deployment, migration, backup/restore, rollback, security, API, and acceptance documents shipped with the source.