

AWRA OPSSHUB · IT, RISK AND AUDIT

AWRA Security Overview

How access, data and evidence are controlled.

Security that travels with the work

AWRA is designed around the work people actually do — moving stock, approving purchases, issuing invoices, managing vendors, syncing mobile devices and reviewing finance records — so its controls sit on those actions rather than in a separate policy folder.

Control layers

Organization isolation

Every record is bound to its organization. A request that carries no organization context returns nothing rather than everything.

Identity

Single sign-on, passwordless email links and passwords with multi-factor authentication. Every sign-in path runs the same MFA and verification checks.

Devices and sessions

Trusted devices, inactivity timeouts, force logout and remote revocation, including for the mobile app.

Permissions

Role-based permissions decide which screens, actions and modules each person can use — down to who may download a stored attachment.

Audit trail

Approvals, impersonation, device activity and sensitive changes keep who, when and what for later review.

Delivery hardening

HTTPS throughout, a content security policy with per-request nonces, verified payment webhooks, and redirects that refuse to send a user off-site.

How a sensitive action is controlled

1 Authenticate the user

Verified identity, MFA policy, password rules and session checks protect the way in.

2 Authorize the action

Roles, permissions, plan and organization policy decide what the user can actually do.

3 Record the event

The action and its context are written to the audit trail.

4 Respond

Administrators can revoke device trust, end sessions and review activity when something looks wrong.

Offline work stays controlled

- Offline unlock is limited to devices that previously signed in and were trusted, for a one-day window.
- Offline actions queue on the device and are validated by the server when they reconnect — the device never has the last word.
- GPS proof can be required on movements where location matters.

Documents for your review

- Trust center, security whitepaper and compliance status: awraops.com/trust-center
- Data processing agreement and privacy policy, available to every customer.
- Responsible disclosure policy for security researchers.
- Uptime commitments are set out in customer SLA terms.

Next step

Request a written quotation for management approval at **awraops.com/request-a-quote**, book a walkthrough at **awraops.com/request-demo**, or start a 30-day trial with every module switched on at **awraops.com**.

info@awraops.com · +254 711 497 488 · Ngong Road, Karen, Nairobi, Kenya