BACKBONE ATLAS

Data Controls & Evidence

For each promise we make about your data: the mechanism that enforces it, and how you can verify it independently. Every item below is enforced in the software today, not asserted in a policy.

WHAT WE PROMISE	HOW IT IS ENFORCED	HOW TO VERIFY IT
Records cannot be deleted, only their status changed	Requisitions, POs, invoices, contracts, bids, suppliers and users are never hard-deleted — the code has no DELETE for them; they move through states. Users are soft-deleted so the trail still resolves to a name.	Code review: no `DELETE FROM` for those tables. Attempt a delete in the product — only a status change is possible.
Evidence stays put once a decision rests on it	Attachment removal is gated to open/draft or self-owned content. Once a requisition is approved its documents are locked; a bidder's submitted documents are kept.	Approve a requisition, then try to remove its document — refused. Inspect the attachments gate.
The activity log cannot be edited or erased	audit_log is a SHA-256 hash chain (each row seals the previous). Database triggers reject any UPDATE or DELETE. Every write goes through one logging function (verified by test).	Run `db.verify_audit_chain()` — reports intact/first-broken row. Attempt an UPDATE/DELETE on audit_log — rejected by the DB.
Tampering is detectable even with database access	The log's length and head hash are anchored off-site every hour into immutable storage (Backblaze Object Lock), so a wholesale re-sealed rewrite is caught, not just a single edit.	Inspect control.db audit_anchors and the immutable off-site copies. restore-test verifies the chain and anchor on every restore.
No single administrator can remove another	Removing / deactivating / demoting an admin (when >1 admin exists) becomes a request a different admin must approve; the requester cannot approve their own; the last admin is never removable.	As one admin, attempt to remove another — the action is held at /settings/admin-approvals for a second admin. Both request and decision are in the sealed log.
Configuration deletions are recoverable and attributable	Deleting a delegation, approval rule or the authority schedule records the full removed content into the tamper-evident log before deleting.	Delete a rule, then find its full prior content in the activity log entry.
Your data stays in Canada, isolated per company	Hosted in DigitalOcean Toronto. One separate SQLite database file per company — no shared multi-tenant table. Cross-tenant isolation verified by penetration test.	Hosting-region attestation; architecture review; independent penetration-test report.
Encrypted at rest, in transit, and field-by-field	AES-256 LUKS full-volume encryption; Fernet field-level encryption of bank details, MFA secrets and connector credentials with keys held OUTSIDE the database; TLS + HSTS.	Volume/key configuration review. Check response headers for HSTS. A copied database file yields no readable secrets.
Only the right people can act; MFA can be required	Role-based access control (self-approval blocked, finance-only payment). TOTP two-factor can be required for all users or admins. Enforced password policy; immediate lock-out.	Role matrix review; attempt self-approval (blocked). Set MFA to required and confirm enforcement.
Backups are hourly, off-site, and proven to restore	Hourly verified SQLite backups; an off-site copy is client-side-encrypted before it leaves (the provider stores only ciphertext); scheduled restore tests open every database.	restore-test logs; rclone shows only ciphertext at the provider; recovery point about one hour.
Ransomware cannot reach or poison the backup history	Off-site backups use immutable, versioned storage (Backblaze Object Lock) — a written copy cannot be altered or deleted, even with a stolen key — plus a founder-held copy kept off the cloud entirely. Post-infection snapshots sit alongside, never replace, the clean older ones.	Object Lock / versioning settings on the bucket; the off-cloud copy; restore to a pre-infection point in a rehearsed 30-60 min recovery.
Your data is yours to take	An administrator can export the entire workspace to open CSV files from inside the product; the per-company database makes return or deletion a clean, complete operation.	Run Settings -> Export workspace; open the CSV/manifest ZIP.

WHAT WE PROMISE	HOW IT IS ENFORCED	HOW TO VERIFY IT
Host monitoring and intrusion detection	auditd (targeted rules on keys, code, identity, persistence), AIDE file-integrity, rkhunter, Lynis, reviewed in a nightly report; fail2ban, firewall, WAF in front.	Nightly security report file; audit rules on the host.

WHAT WE DO NOT CLAIM

Stated plainly, not hidden: no SOC 2 / ISO 27001 certification; a single Canadian region with an honest 99.5% availability target (fast recovery, not zero-downtime failover); operator support access exists but is restricted and logged like everything else. Your data is never sold, shared, or used to train models.
