SaccoWorks — Security & Data Protection Pack

Vendor: eLiveCode Solutions Limited · **Product:** SaccoWorks · **Version:** July 2026

This pack describes the security posture of the SaccoWorks platform for procurement due diligence. Status is stated honestly: **In place** (operating today), **Partial** (core in place, being formalized), or **Planned** (committed on the roadmap). Nothing is overstated.

1. Architecture overview

- **Deployment:** Cloud-hosted, browser-based (ASP.NET / .NET Framework 4.8) with a companion .NET 8 REST API for mobile and integrations. Member self-service via web portal and Android app.
- **Multi-tenancy:** One platform serves many SACCOs. **Every data record and query is scoped by a tenant `CompanyID`** — tenants cannot see each other's data. *(In place)*
- **Payments:** M-Pesa (STK / C2B / B2C) and bank disbursements are handled through a dedicated payment bridge with signed callbacks. *(In place)*

2. Identity & access management

Control	Status	Detail
Role / rights based access control	**In place**	Per-user roles and menu/function rights (`UserManagement` , tenant menu rights).
Password hashing	**In place**	Passwords stored hashed (PBKDF2 / BCrypt), never in clear text.
Session management	**In place**	Server-side session context; sign-out and timeout.
Attack-surface control	**In place**	`LegacySurfaceGuard` blocks any page/handler not explicitly approved for a tenant — unused/legacy screens cannot be reached.
Multi-factor authentication (admins)	**Planned**	Mandatory MFA for administrators is on the near-term roadmap.
Password policy & periodic access reviews	**Partial**	Strong-password rules in place; scheduled access-review reporting being formalized.

3. Auditability

Control	Status	Detail
Audit trail of key actions	**In place**	`AuditLog` / `Sacco_AuditTrail_Sp` record user, action, description and timestamp for postings, changes and admin activity.
Financial posting trail	**In place**	Double-entry GL with per-transaction references; reconciliation reporting (`sp_Report_GLReconciliation`).
Immutable / tamper-evident logs	**Planned**	Append-only / write-once hardening of audit logs is planned.

4. Data protection

Control	Status	Detail
Encryption in transit	**In place**	HTTPS/TLS for the application, portal, API and payment callbacks.
Tenant data separation	**In place**	Logical isolation by `CompanyID` across all tables and queries.

Control	Status	Detail
Credential management	**In place**	Production credentials and application machine key are rotated and kept out of source control; the live `web.config` is never overwritten by deployments.
Encryption at rest	**Planned**	Database/disk-level encryption at rest to be enabled/confirmed with the hosting tier.
Kenya Data Protection Act alignment	**Partial**	Access control, audit and consent capture in place; a formal DPA controls pack (data map, retention, subject-request process) is being documented.

5. Backups & recovery

Control	Status	Detail
Database backups	**In place**	Regular SQL Server backups of tenant data.
Off-site / automated backups	**Partial**	Being standardized to automated off-site storage with defined retention.
Restore testing	**Planned**	Quarterly restore tests to be scheduled and evidenced.
RPO / RTO targets	**Planned**	Formal Recovery Point / Recovery Time Objectives to be published in the contract.

6. Infrastructure & change management

Control	Status	Detail
Staged deployment	**In place**	Changes are deployed to a staging path first, then production (release control).
Separate production & test **databases**	**Partial**	Staging isolates file/URL testing; fully separate non-prod data environment being finalized.
Monitoring & alerting	**Partial**	Operational monitoring in use; formal alerting thresholds being documented.
Source control & release process	**In place**	Versioned source control; changes reviewed before release.

7. Testing & assurance

Control	Status	Detail
Functional / regression testing	**In place**	Pre-release testing on staging.
Vulnerability scanning	**Planned**	Monthly automated scans to be introduced.
Independent penetration testing	**Planned**	Annual third-party penetration test to be commissioned.

8. Incident response

Control	Status	Detail
Escalation process	**In place**	Defined support escalation (desk → engineer → development → management).
Customer notification	**Partial**	P1/P2 status updates provided; formal notification SLA being documented.
Root-cause analysis	**In place**	RCA summary provided for P1/P2 incidents.

9. Service levels

See the separate **SLA & Support Matrix**. Committed uptime target **99.5%/month** (excluding scheduled maintenance and third-party outages); support response targets by priority; **≥95%** SLA achievement target.

Summary for evaluators

SaccoWorks operates with tenant isolation, role-based access, hashed credentials, TLS in transit, audit trails and staged deployment **today**. The honest near-term hardening items — mandatory MFA, encryption-at-rest confirmation, automated off-site backups with restore tests and published RPO/RTO, and independent penetration testing — are committed on the roadmap and can be written into the contract as milestones.
