ASIRI Security Pack

Current security posture, operating boundaries, and assurance roadmap for buyer review.

PUBLIC v2026.05 May 2026

Audience

CTOs, CISOs, procurement teams, DPOs, and founders preparing for enterprise review.

Scope and disclaimer

This pack summarizes ASIRI's current security posture and assurance roadmap. Certification, audit, and enterprise-only controls are only claimed where explicitly labeled.

Security posture summary

ASIRI is designed as a privacy operations platform for NDPA programs, evidence workflows, DPIA records, DSR handling, breach readiness, and Trust Center publishing. The platform favors tenant separation, least-privilege access, auditable workflows, and controlled evidence disclosure.

- Live controls focus on application access, data protection, operational logging, and vendor review.
- Scoped Enterprise controls are reviewed during enterprise onboarding before being represented as available.
- Roadmap items are included to help buyers understand direction without treating planned work as current capability.

Data residency and hosting

Primary hosting model	Cloud-hosted application with regional deployment planning for Nigerian and enterprise data-residency requirements.
Customer content	Compliance records, policy evidence, DPIA notes, DSR workflow data, and Trust Center materials uploaded or generated by customer teams.
Residency posture	Designed for clear data-location review during procurement; dedicated residency commitments require enterprise scoping.

Encryption and keys

In transit	TLS is expected for production traffic across public application endpoints and service connections.
At rest	Production data stores are designed to use managed encryption-at-rest capabilities provided by the hosting and storage layers.
Key ownership	Customer-managed keys are treated as an Enterprise review item and are not claimed as generally available in this version.

Tenant isolation

ASIRI is built around organization-scoped records and workflows. Tenant isolation is enforced at the application and data-access layer, with workspace boundaries used for evidence, policies, tasks, approvals, and Trust Center content.

- Organization context is required for customer records and workflow actions.
- Administrative access is limited to operationally necessary support and security tasks.
- Enterprise architecture review can cover tenant controls under NDA when required.

Access control

Customer users	Role-based access patterns support operational separation between administrators, reviewers, contributors, and viewers.
Staff access	Staff access is intended to follow least-privilege operating practices and documented support need.
Authentication	Standard authentication is available; SSO and advanced identity controls are scoped for Enterprise review where applicable.

Auditability

ASIRI records compliance activity so teams can reconstruct decisions, evidence changes, and review status. Logs and evidence trails are designed for workflow review, not as a substitute for a forensic audit report.

- Evidence timelines show review progress and material updates.
- DPIA and DSR records preserve reviewer context and status movement.
- Exported artifacts include version and sample-data labeling where applicable.

Incident response

Operating model	Incident response procedures are aligned to triage, containment, customer impact assessment, remediation, and post-incident review.
Notification posture	Breach-notification workflows are designed to support NDPA-aligned internal review and customer communication.
Customer role	Customers remain responsible for their own legal, regulator, and data-subject notification decisions.

Sub-processors

ASIRI maintains a controlled vendor review posture for infrastructure, product operations, and support tooling. A current sub-processor list and notification approach can be reviewed through the procurement request process.

Public detail	High-level processing categories are shared publicly.
Procurement detail	Specific vendor review artifacts are available through buyer diligence when appropriate.

Assurance roadmap

Live	Security posture documentation, access-control review, controlled evidence exports, and privacy workflow audit trails.
Scoped for Enterprise	SSO, dedicated residency commitments, advanced architecture review, and deeper security questionnaires.
Planned	Expanded control mappings, stronger automated freshness signals, and richer Trust Center subscriber notifications.
Enterprise-only	Customer-specific control evidence and architecture sessions under NDA.

Security contact

Security questions, vulnerability reports, and procurement evidence requests can be routed to security@asiri.ng or through the ASIRI contact-sales workflow.