

Data security policy

Security requirements for ASMRAF records, access and service providers.

Draft for ASMRAF review - Version 0.2 - 14 October 2026

Prepared for the South African launch. These are proposed rules, not confirmation that legal arrangements, staff or services are in place.

1. Scope and responsibility

This proposed policy covers registration, identity, verification, complaint and traceability records, including copies and backups. Appoint accountable security and privacy owners. Keep an inventory of systems, data, operators and administrators. Classify identity documents, exact mine locations and safeguarding reports as restricted. Supabase provides platform controls; ASMRAF remains responsible for its configuration and use.

2. Access and separation

Use named accounts, least privilege and multi-factor authentication for staff and administration. Grant authority separately from ordinary sign-in and remove access when duties end. Keep ASMRAF verification access separate from MinePay commercial access. Review privileged access regularly. Shared project administration can cross application boundaries and must be expressly assessed before real identity data is collected.

3. Storage and disclosure

Keep personal records in private schemas or storage buckets. Deny anonymous access and enforce explicit authorisation on each operation, including exports and document downloads. Use encrypted transport and platform encryption at rest. The present raw national-ID field is not separately encrypted from database administrators; decide whether to minimise it or add independently managed field encryption before live collection. Do not put service credentials in browser code, logs or downloadable files.

4. Secure operation

Separate test fixtures from real records. Validate input, limit requests, record administrative changes and avoid logging raw identity data or secrets. Review database functions, policies and storage rules after changes. Keep dependencies updated, manage secrets centrally and test denial as well as permitted access. Assess any new chatbot or messaging provider before sending it personal information.

5. Recovery and incidents

Approve backup, deletion and recovery procedures and test restoration with documented results. A backup setting alone is not proof of recovery. On suspected compromise, contain exposure, preserve evidence, assign an incident lead, assess affected people and remediate. The Information Officer must determine required notices under POPIA and other applicable duties; do not wait for complete certainty before escalating. Do not promise that every incident has the same legal deadline.

6. Retention and assurance

Adopt a purpose-based retention schedule with deletion, anonymisation and legal-hold rules, including backups. Confirm hosting locations, operator contracts and international transfers. Keep evidence of access reviews, restore tests, incident exercises and staff training. Review this policy annually and after significant incidents or architecture changes. The NIST functions provide a useful planning structure; this is not a claim of NIST certification.

Before adoption

Approve administrator access and key management, verify project region and operator terms, implement retention/deletion, complete restoration and incident tests, and approve the security release review.

Proposed accountable role: ASMRAF security lead and Information Officer. Record named appointments and an adoption date before operation.

References

[NIST Cybersecurity Framework 2.0](#)

[Supabase shared responsibility](#)

[Information Regulator security compromises](#)

References inform this draft; they do not imply endorsement or certification of ASMRAF.