

Policies and documents

ASMRAF / South African launch

Draft review pack - 14 October 2026

ASMRAF is funded only by corporate, industry and individual memberships. Registration, MUCC codes and verification are free for miners.

Read this pack

These 13 documents describe proposed rules and the current presentation and testing website. They require ASMRAF adoption, named responsibilities and completion of the legal and operational arrangements listed in each document. Real registration remains closed.

1. Due diligence policy
2. Privacy notice
3. Child and forced labour policy
4. Health and safety policy
5. Anti-bribery policy
6. Conflicts of interest policy
7. Data security policy
8. Complaints and appeals procedure
9. Website and registration terms
10. Approved buyer participation terms
11. MUCC specification
12. MUCC provider use terms
13. Example mine record

No payment or mineral-supply guarantee is created by a MUCC code. MinePay is a technology provider and has no verification authority.

Due diligence policy

How ASMRAF proposes to identify risks, assess evidence and make independent verification decisions.

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. Purpose and scope

This proposed policy applies to ASMRAF staff, assessors and verification decision-makers, and sets expectations for participating mines and providers. It supports responsible mineral sourcing; it does not replace government licences, the buyer's own checks or legal duties. Registration, MUCC codes and ASMRAF verification are free to miners. Corporate, industry and individual memberships are ASMRAF's only funding sources.

2. The verification file

Create one controlled file per mine, linked to its MUCC code. Identify the applicant, their authority to represent the mine, the mine's location and lawful operating rights. Record sources, dates, reviewer and limitations. Confirm permissions for the specific activities and minerals, rather than treating any permit as permission for every activity. A provisional code records registration only.

3. Risk assessment

Use a documented risk assessment covering serious human-rights abuses, child and forced labour, armed-group involvement, abusive security practices, bribery, false origin claims, money laundering, taxes and royalties. Also assess safety, environmental harm and community concerns. Compare official records, interviews, site observations and lot evidence. An assay identifies material characteristics; it does not by itself prove lawful origin or ownership.

4. Decisions and corrective action

Record each finding, severity, evidence and proposed action. Credible serious-abuse or armed-group risks require escalation and suspension of verification or associated sourcing recommendations while assessed; an ordinary improvement plan is not a reason to overlook them. For remediable gaps, agree a named action owner, deadline and evidence for closure. Do not close a finding because a document was uploaded. Record the independent review and reasons for every outcome.

5. Independence and continuing checks

Only expressly authorised ASMRAF personnel may change verification status. Anyone with a financial or personal interest must disclose it and step out. MinePay is a technology provider and has no verification vote. Reassess after material changes, serious incidents or credible complaints. When status changes, record whom to notify, what they need to know, delivery and follow-up; do not disclose confidential allegations unnecessarily.

6. Accountability

The proposed approach follows the OECD sequence of management systems, risk assessment, response, independent audit and reporting. Appoint qualified reviewers and an independent auditor before describing those arrangements as operational. Publish proportionate summaries without personal identities or precise mine locations. Keep a decision log, corrective-action register and complaints route; review this policy annually and after a serious incident.

Before adoption

Appoint the verification lead and decision body, approve country-specific checks, commission independent audit arrangements and adopt the records schedule.

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

References

[OECD minerals due diligence guidance](#)

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

Privacy notice

How the shared demo works, what it stores and the proposed arrangements for real registration.

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. Current service and contact

ASMRAF plans to register in Abu Dhabi, United Arab Emirates, and launch operations first in South Africa. Registration has not been completed: the legal name, legal form, registration number, address and accountable privacy contact remain to be confirmed. This notice does not claim that ASMRAF is registered in ADGM or any particular free zone. Contact info@asmraf.org with a privacy enquiry; do not email identity documents. Real mine registration remains closed. The site offers a working demonstration using fictional mine names.

2. What the shared demo stores

The demo asks for a fictional mine name and South Africa as the country. Supabase stores the DEMO code, the labelled mine name, country link, random retry identifier, creation date and expiry date. It does not request or send your name, national ID, passport, contact number, street address or device location. No registration data is kept in browser local storage by this demo. Anyone with the complete demo code and matching mine name can retrieve the limited demo record and use it in the MinePay test journey, so use fictional information only. Opening a MinePay account is a separate process with its own notice.

3. Information proposed for registration

The current design asks for name, national ID or passport number, mine name, country and mine address, with optional contact details afterwards. These would support identity and authority checks, duplicate prevention, mine identification and application updates. Before launch, ASMRAF must document a lawful basis and necessity for each field, including whether a less intrusive identity check can replace retaining the raw number. A consent box alone does not resolve those duties.

4. Access and sharing

Demo data is held in a restricted database schema with a minimal mine-name, code, country and Demo-status mirror in MinePay's shared registry. Public functions allow creation and code-plus-name lookup of fictional records only; they do not expose a list of registrations or identity data. Demo records do not represent ASMRAF verification. The real-registration design separately keeps identity information in a private schema inaccessible to ordinary website and MinePay users. Individually authorised verification staff and privileged technical administrators would need controlled access. MinePay has no verification authority.

5. Security and international hosting

The connected Supabase project is in the eu-central-1 (Frankfurt) region. Supabase documents encryption in transit and at rest; database privileges and row-level security restrict direct table access. Privileged administrators can read stored values. Hosting and API providers may process IP addresses and security logs to operate the service. Before real collection, confirm operator contracts, backup locations and safeguards for international transfers from South Africa and the UAE. A planned Abu Dhabi entity does not mean data is stored in Abu Dhabi.

6. Retention and your choices

Demo codes stop working in MinePay 30 days after creation. Expiry is not automatic deletion: demo records and linked test history remain until the pilot records are reviewed and removed or anonymised by an administrator. No real identity-data retention period has been approved. Before live registration, publish justified periods and deletion procedures for identity details, verification evidence, contact information, history, logs and backups. If you accidentally enter personal information into the demo name, contact info@asmraf.org with the demo code and request correction or removal; do not send further identity documents by email.

7. Questions and complaints

Send a request headed Privacy to info@asmraf.org with a safe way to reply and a MUCC code if relevant, without attaching ID. ASMRAF must establish proportionate identity checks, an accountable case owner and legal response deadlines before launch. South African complaints can also be raised with the Information Regulator through its official website. Version privacy-2026-10 is a review draft, not an approved notice for live collection; material changes must be versioned and communicated.

8. Applicable privacy arrangements

South African operations require a POPIA assessment. The UAE regime depends on the final entity, place of establishment and activities; ADGM has a distinct data-protection framework. Confirm the applicable regime and responsible entity before real collection. These draft pages do not assert that incorporation or compliance has been completed. No advertising analytics or conversational assistant is configured. External email, WhatsApp sharing and website links use the selected third-party service under its own terms.

Before adoption

Confirm the legal responsible party, Information Officer, mailbox, lawful purposes and bases, hosting and transfer arrangements, retention/deletion schedule and rights-handling process. Complete POPIA review before real registration.

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

References

[Protection of Personal Information Act](#)

[Information Regulator](#)

[Supabase shared responsibility](#)

[UAE government: data protection](#)

[ADGM Office of Data Protection](#)

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

Child and forced labour policy

Protecting children and workers, with a practical response to suspected abuse.

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. Who this protects

This proposed policy applies to mines seeking ASMRAF verification, their contractors, labour brokers, assessors and ASMRAF personnel. It prohibits child labour and all forced, trafficked or bonded labour. As a proposed ASMRAF participation rule, nobody who is a child may undertake hazardous mining or processing work. Any stricter applicable rule also applies. This rule is not a statement that every country has identical labour law.

2. Checks before verification

Assess recruitment methods, age-verification practices, working hours, wages, freedom of movement and ability to leave employment. Interview workers privately and safely, with suitable language support. Check for withheld identity papers, recruitment debts, threats, coercion, wage withholding, exploitative deductions and restrictions on leaving. Do not treat a signed declaration as sufficient evidence or collect children's identity documents casually.

3. Responding to a concern

Prioritise immediate safety. Do not confront a suspected trafficker or expose a complainant to retaliation. Escalate to a trained safeguarding lead, make a factual confidential record and obtain competent advice on mandatory reporting and safe referral. Where someone is in immediate danger, contact appropriate local emergency services. Do not promise confidentiality that prevents a legally required protective disclosure.

4. Protective remediation

Do not respond by simply dismissing a child or withholding wages. Work with appropriate protection services on safe removal from hazardous work, education and family support, considering the child's interests. For forced labour, prioritise safe exit, return of documents, access to earned wages and suitable support. Involve affected people safely in remedy planning. Keep the names and locations of vulnerable people out of public reports.

5. Verification consequences

Credible serious-abuse concerns must be escalated and can prevent or suspend verification. A routine corrective-action plan cannot justify continued abuse. Any restoration requires independent evidence that the harm has stopped, remedial steps are effective and recurrence risks are addressed. Buyers and providers receive only the status and relevant restriction information they lawfully need.

6. Reporting and oversight

Use info@asmraf.org to request a safe reporting route, without sending sensitive case files to a general inbox. A person may ask that their identity be withheld, although ordinary email is not anonymous. Do not penalise good-faith reports. Keep a restricted case log, referral record and follow-up review. The safeguarding lead must arrange staff training and review this policy annually and after any serious case.

Before adoption

Appoint a safeguarding lead, establish South African referral and emergency arrangements, confirm reporting duties and secure case access, and train assessors.

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

References

[ILO child labour standards](#)

[ILO mining resources](#)

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

Health and safety policy

A practical safety baseline for assessment visits and mines seeking verification.

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. Responsibilities

This proposed policy covers ASMRAF staff and visitors, assessors and participating mines. The mine operator remains responsible for lawful, safe operations. ASMRAF verification does not replace a statutory inspection, engineering design or a competent person's approval. Assessors must not present themselves as qualified for tasks outside their competence.

2. Plan before a visit

Agree the visit scope, host, access route, emergency contacts and site induction. Review known hazards and stop conditions. Use a suitable check-in arrangement and reliable means of communication. Do not enter unstable excavations, unsupported underground workings, confined spaces or hazardous plant areas without competent authorisation and the required controls. A verification target never justifies unsafe entry.

3. Assess the actual risks

Review ground stability, excavation and shaft access, machinery guarding, lifting, electricity, vehicles, explosives, dust and silica, noise, heat, chemicals, water, sanitation, waste and tailings. Consider workers, neighbours and vulnerable people. Record the hazard, exposed people, controls and remaining risk. Eliminate hazards where possible; use engineering and work controls before relying on protective equipment alone.

4. Worker protection

Require understandable training, appropriate protective equipment, maintained tools and a way to raise concerns without retaliation. Workers must be able to move away from imminent danger and report it. Confirm safe water, first aid, emergency arrangements and communication suited to the site's location. Specialist hazards such as explosives, hazardous chemicals or cyanide need competent, legally compliant controls; this document is not an operating instruction.

5. Incidents and corrective action

For immediate danger, stop the assessment or affected activity and seek appropriate emergency help. Record facts, preserve evidence safely and make legally required reports. Classify findings by severity, assign actions and verify closure through evidence. Do not mark a mine safe because safety equipment was bought or a form completed. Serious unresolved risks prevent a favourable verification decision.

6. Records and review

Maintain induction, training, inspection, incident and corrective-action records with restricted access to health information. Review recurring causes with workers and management. The safety lead checks that actions have been completed and independently reviewed where needed. Reassess after major changes or incidents; review the policy annually.

Before adoption

Appoint the safety lead, establish competent-assessor criteria, country-specific legal checks, emergency arrangements and site-visit procedures.

Proposed accountable role: ASMRAF safety lead and each mine operator. Record named appointments and an adoption date before operation.

References

[ILO Safety and Health in Mines Convention](#)

[ILO mining resource kit](#)

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

Anti-bribery policy

Keeping registration, verification and membership free from improper influence.

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. Core rule

Under this proposed policy, no person acting for ASMRAF may offer, request, promise or accept an improper benefit to influence a decision. This includes money, gifts, travel, employment, discounts, donations or favours, directly or through someone else. It applies to staff, assessors, committee members, contractors and agents.

2. Free registration and independent decisions

Miners pay nothing to register, receive a MUCC code or undergo ASMRAF verification. Nobody may charge to accelerate, activate or upgrade a code. Membership funding is separate from verification. A membership purchase, sponsorship claim, founding-member relationship or commercial introduction gives no preferential assessment or decision-making right.

3. Gifts and hospitality

Do not accept cash or cash equivalents. Decline benefits from an applicant or interested party while their decision is pending. Other gifts or hospitality need prior written approval by a person without a conflict, with purpose, value, parties and decision logged. In the absence of an approved limit, decline rather than assume permission. Do not split expenses or use personal accounts to evade controls.

4. Third parties and payment requests

Check the identity, authority and role of agents and suppliers, and document their work and payment terms. Reject unexplained commissions, false invoices and requests to redirect payments without independent verification. Do not make facilitation payments. If a demand is accompanied by an immediate threat to safety, prioritise safety, preserve a factual record and report it promptly; never conceal it as an ordinary expense.

5. Reporting and response

Report concerns to the integrity lead through a secure route; info@asmraf.org can be used to request that route. If the concern involves the lead, an unconflicted governing-body member must handle it. Preserve evidence, limit access and protect good-faith reporters from retaliation. Investigations must be fair and separate from those implicated. Make external reports when legally required.

6. Controls and accountability

Keep gifts, expenses, conflicts and incident registers. Use named authority and a second check for sensitive approvals. Apply proportionate consequences under lawful employment and contractual procedures. Train personnel before they work with applicants and review risks, incidents and the policy at least annually. Publish factual outcomes only when safe and lawful.

Before adoption

Appoint the integrity lead and alternate escalation contact, approve gifts/expenses rules and secure reporting channels, and adopt training and investigation procedures.

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

References

[UNODC Business Integrity Portal](#)

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

Conflicts of interest policy

How interests are declared, reviewed and kept out of verification decisions.

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. What counts as a conflict

This proposed policy covers actual, potential and reasonably perceived conflicts. Examples include ownership, employment, fees, debts, family or close personal relationships, gifts and competing advisory roles involving a mine, buyer, provider or applicant. A person may have a conflict without acting dishonestly; the duty is to disclose and manage it.

2. Declare before acting

Each staff member, assessor and decision-maker must declare relevant interests on appointment, annually, before every affected case and whenever circumstances change. Record the organisation or relationship, its nature, affected work and date. Do not publish private financial or family details unnecessarily. Maintain a controlled register and a proportionate public summary after approval.

3. Independent assessment

An unconflicted person decides whether reassignment, recusal or another control is required. The person declaring the interest does not approve their own management plan. Where independence cannot be protected, do not proceed with the assignment. Record the decision, reviewer and reasons.

4. Recusal in practice

A recused person must not review the evidence, influence colleagues, vote, approve status changes or receive confidential case material beyond what is necessary. Identify a replacement with suitable competence and record the remaining decision authority. If the committee cannot make a valid decision without the conflicted members, escalate or defer the case rather than manufacture approval.

5. MinePay and funding separation

MinePay is a technology provider and takes no part in ASMRAF verification decisions. Corporate, industry and individual memberships are ASMRAF's only funding sources. Membership, commercial fees and referral opportunities must not determine a mine's verification outcome. Founding-member recognition does not automatically grant assessment or governance authority.

6. Reporting and review

A person can question independence without retaliation. Request a confidential reporting route through info@asmraf.org; an unconflicted governing-body member must handle allegations involving the normal reviewer. Record the concern and action, restrict unnecessary access and review affected decisions if a conflict was undisclosed. Review this policy annually and following significant governance changes.

Before adoption

Confirm the governing body, decision authority, quorum and alternate reviewers; collect declarations and establish the interests register.

Proposed accountable role: ASMRAF governing body. Record named appointments and an adoption date before operation.

References

[UNODC Business Integrity Portal](#)

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

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.

Complaints and appeals procedure

A proposed route for concerns about mines, staff conduct or verification decisions.

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. Who can raise a concern

Miners, workers, communities, buyers and other affected people may raise concerns. Good-faith complaints must not lead to retaliation or automatic rejection of a mine. A complaint addresses a concern or conduct; an appeal requests reconsideration of a decision. Neither creates an automatic favourable outcome.

2. Make contact safely

Email info@asmraf.org with a short description, relevant MUCC code, dates and a safe way to reply. Do not send ID documents or sensitive evidence until a secure route is agreed. Email reveals the sender's address and is not anonymous. A representative may assist with permission. Phone, WhatsApp, a staffed web assistant and an anonymous reporting service are not yet operational.

3. Log and triage

The proposed process assigns a case reference, acknowledges receipt and checks immediate safety, safeguarding, fraud and privacy risks. Tell the person who will handle the case and the expected update date. Response targets and staffing still need approval; the website does not promise round-the-clock human support. Emergencies should go to appropriate local emergency services.

4. Review and decide

Assign a reviewer without a conflict, seek necessary evidence fairly and keep personal details restricted. Record findings, reasons, action owners and follow-up. Explain the outcome in plain language, including any limits on what can be disclosed. An appeal should be reviewed by someone not responsible for the original decision. Do not assert an appointed arbitrator until one is agreed.

5. Close and learn

Record communication and whether remedies were verified, rather than closing a case when an email is sent. Explain any further review route. Do not invent an appeal deadline while the rules remain unapproved. Maintain a restricted complaints register and review trends without publishing identities.

Before adoption

Confirm case owner and independent appeal route, test the mailbox and secure evidence channel, and approve response targets and appeal rules.

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

Website and registration terms

Proposed terms explaining the review website and the limits of a MUCC code.

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. Review website

This website is open for presentations and testing. Test registrations are stored centrally, can be retrieved from another device and can be used in the MinePay test journey for 30 days. Use only fictional mine names. Real mine registration is not open. These draft terms are not a signed participation agreement.

2. The MUCC code

A Provisional MUCC code identifies a registration pending checks. It is not a licence, verification certificate, ownership proof, safety guarantee or permission to sell. A Certified status would record an authorised ASMRAF decision with defined scope and current validity; the underlying government permissions and transaction checks remain necessary.

3. Applicant responsibilities

Only submit accurate information you are entitled to provide. Represent a mine only with its authority. Do not use another person's documents or try to bypass checks. ASMRAF may ask for corrections or further evidence through approved channels. A person must not be rejected solely for asking for help or raising a good-faith complaint.

4. Fees and commercial activity

Miner registration, MUCC codes and ASMRAF verification are free. ASMRAF is funded only by corporate, industry and individual memberships. Membership fees are stated in US dollars; payment details, billing period and tax treatment require confirmation before accepting subscriptions. ASMRAF does not buy minerals or handle payments. MinePay is a technology provider, and separate commercial arrangements apply to a sale.

5. Privacy and fair use

Read the privacy notice before any future real submission. Do not scrape private records, impersonate staff, upload harmful files or claim that a draft document is an approved certificate. External websites have their own terms. Raise complaints through the published procedure. Legal entity details, governing law, dispute arrangements and any enforceable limitations require South African legal review before adoption.

6. Legal identity and planned establishment

ASMRAF plans to register in Abu Dhabi, United Arab Emirates. Its registered legal name, form, number, office address and governing-law arrangements are pending. South Africa is the first planned operating market. No claim is made that the entity is already incorporated, licensed in ADGM or registered in another free zone. Final terms and privacy responsibilities must be reviewed against the confirmed establishment and operating arrangements before real registration opens.

7. Demo use and its limits

Demo codes begin DEMO-MUCC and demo mine names begin DEMO. Keep both to find the record on another device or enter it in MinePay. Do not enter ID numbers, real mine addresses or confidential material into a demo name. Demo records are not verified mines and cannot create real payment instructions. Expiry does not delete linked test history. Production registration, certification, actual sales and real payouts require the separate live-service requirements to be met.

Before adoption

Confirm the contracting legal entity and South African legal terms; align registration consent and membership agreements with the final adopted versions.

Proposed accountable role: ASMRAF legal and programme leads. Record named appointments and an adoption date before operation.

Approved buyer participation terms

Proposed requirements for buyers using ASMRAF-linked mine and lot information.

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. Admission and scope

This draft does not approve any buyer. Assess the applicant's identity, beneficial ownership where necessary, relevant licences, sanctions and risk profile, and the intended minerals and jurisdictions. Record approval scope and authority. Participation does not replace the buyer's legal, sourcing, tax, import or export obligations.

2. Before each purchase

Check the mine's current status and relevant operating rights, the seller's authority, lot identity, quantity, assay and custody evidence. Resolve mismatches before relying on the record. A code alone does not prove every claim about a consignment. Do not treat a provisional, suspended or withdrawn status as a Certified verification.

3. Confidential information

Access only the information authorised for the transaction and purpose. Keep identities, exact locations and documents confidential, restrict access within the buyer's organisation and prohibit onward use unrelated to due diligence. A confidential seller label does not remove the need for true legal identities in required legal and compliance records. MinePay's confidential fee arrangements are not automatically buyer-visible.

4. Commercial and settlement records

The miner sells to the buyer; ASMRAF verifies and MinePay may facilitate through its technology. Separate contracts must identify the actual parties, price, costs, terms, invoice and payment responsibilities. Creating an invoice or approving a contract is not evidence that a miner was paid. Payment records must be supported by the relevant provider or bank confirmation.

5. Changes and breaches

Report material changes, suspected fraud and serious sourcing risks promptly through agreed secure channels. ASMRAF may restrict access or participation after a documented review, with an appropriate appeal route. Data-access scope, retention, fees if any, liability and dispute terms must be settled in a signed agreement before operational access.

Before adoption

Approve buyer admission criteria, authorised data views and signed terms; identify competent reviewers and supported launch activities.

Proposed accountable role: ASMRAF programme and legal leads. Record named appointments and an adoption date before operation.

References

[OECD minerals due diligence guidance](#)

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

MUCC specification

An implementation draft describing identifiers, statuses, records and the separation of verification from commerce.

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. Identifier and scope

Draft version 0.2, dated 14 October 2026. A MUCC identifies one mine registration. The implemented format is MUCC-YYYY-NNNNNN, with a four-digit year and six-digit sequence. Display codes in uppercase and normalise case and surrounding spaces when matching. Existing reserved test identifiers must not be reissued as new registrations. A lot or sale has its own reference linked to the mine code.

2. Allocation and duplicates

Allocate codes on the server in a transaction with uniqueness protection. A retry using the same request identifier and identical payload returns the same result; a changed payload must not silently overwrite the original. A duplicate mine warning needs controlled human review, including possible legitimate differences, rather than granting a second identity automatically.

3. Statuses

Provisional means registered but not verified. Certified records an authorised verification outcome within a defined scope. Suspended means verification cannot currently be relied upon. Withdrawn means the current verification participation has ended. The code remains an historical identifier; changing status does not erase earlier records or prove that a payment occurred. Certificate validity and renewal rules require formal adoption.

4. Private and shared records

The private application holds applicant name, identity number, mine name, address, country, optional contact, consent version and timestamps. The current MinePay mirror is limited to mine identity and status. Identity numbers and contacts must not be added to that mirror. Keep evidence, decision authority and status events under controlled access. Database administrators remain privileged and need separate governance.

5. Decision control and integration

Only specifically authorised ASMRAF verifiers can change status, with an evidence reference, current-record check and audit event. MinePay staff do not inherit that authority. The public label Certified corresponds to the existing registry status value official, which the present MinePay mirror maps to Active; other states remain non-active. This is a limited registry integration, not proof that every custody, messaging or payment service is connected. Consumers must handle stale information and re-check before relying on status.

6. Operational release

Registry allocation and privacy controls have passed isolated tests. Shared test registrations are now stored centrally and recognised by MinePay's mine lookup, with real payments blocked. The real-registration switch remains off. Before real launch, approve privacy and country rules, resolve verifier access and support recovery, and complete end-to-end device testing. Publishing this draft does not create a standards board, accredited assessor scheme or third-party certification. Record future changes with version, date and migration effects.

Before adoption

Approve the governance authority, operational lifecycle and technical contract. Enforce South Africa as the initial server-side issuance scope before public launch.

Proposed accountable role: ASMRAF standards and technical leads. Record named appointments and an adoption date before operation.

MUCC provider use terms

Proposed rules for technology and other providers referencing MUCC records.

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. Non-exclusive participation

Any provider meeting ASMRAF's requirements may apply on the same terms. MinePay is a technology provider under the owner-confirmed non-exclusive agreement dated 9 November 2025. That relationship gives it no role in verification decisions and no automatic right to all private records.

2. Use only authorised data

Agree the purpose, data fields, access method, roles and retention before integration. Authenticate service access, protect secrets and prevent public enumeration of mines or applicants. Use the minimum necessary information and do not copy raw identity data without an explicit lawful purpose and written arrangement.

3. Represent status accurately

Show provisional, certified, suspended and withdrawn states clearly. Record when status was checked and handle service failures without assuming approval. Do not represent a MUCC as a government licence, proof of payment or guarantee of mineral origin. Describe planned capabilities as planned and identify the limits of the evidence.

4. Preserve records and separation

Keep sale, lot, document and settlement references linked without allowing one action to fabricate another. A document upload is not approval; approval is not payment; a payment instruction is not confirmed recipient receipt. Providers may not change ASMRAF verification status or grant themselves verification authority.

5. Assurance and exit

Agree testing, incident reporting, change management, suspension and termination arrangements. On exit, revoke access, return or securely delete records as lawfully required and retain only justified audit evidence. Legal, intellectual-property, service-level and liability terms require a signed provider agreement before operational use.

Before adoption

Approve provider admission and data-sharing agreements, operational contacts and integration acceptance tests.

Proposed accountable role: ASMRAF standards and legal leads. Record named appointments and an adoption date before operation.

Example mine record

A fictional illustration of the records to keep under a MUCC code.

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. Fictional example only

This record is entirely fictional. It is not an anonymised real case, certificate, mine approval or payment confirmation. Reference: EXAMPLE-MINE-001. Mine: Example Mine. Launch country: South Africa. Status: Provisional. No real MUCC is issued by this document.

2. Applicant and permissions

Applicant identity: held in the restricted application file, not shown here. Authority to represent the mine: evidence needed. Right to carry out the intended mining activity: evidence needed. Exact location: restricted. Scope of minerals and activities: to be established through the assessment.

3. Evidence and findings

Licence validation: not completed. Site visit: not completed. Labour and safety review: not completed. Assay and chain-of-custody records: none received. Corrective actions: to be determined after assessment. Do not populate these fields with an example that looks like a completed check.

4. Decision and transaction links

Verification decision: not made. Decision-maker and evidence reference: none. Sale and lot references: none. Buyer agreement: none. Payment instruction: none. Recipient payment confirmation: none. Each event needs its own evidence and timestamp before the status changes.

5. Minimum audit fields

For a real case record the event type, mine and transaction references, record version, actor, source, time, finding and reason for any change. Keep private evidence references separate from public descriptions. Reopening a file must show what was actually saved, who saved it and whether a decision is still outstanding.

Before adoption

Use only as a training illustration. Replace example values with evidence in an authorised case workflow, never in the public website.

Proposed accountable role: ASMRAF verification team. Record named appointments and an adoption date before operation.