KHEPEE

LEGAL DOCUMENT

AML & KYC Policy

How identity verification and anti-money-laundering controls work on the platform, and the division of responsibility between Khepee and the licensed institution.

Publisher	Lacspace Corporation Pvt. Ltd.
Version	1.0
Published	2026-07-30
Last updated	2026-07-30
Status	Takes effect at launch
Sections	5
Clauses	30
Source	khepee.com/legal/aml-kyc-policy

NOT YET IN FORCE

This document is published for review and does not yet bind anyone. It commences on the date the Khepee lending service goes live with a licensed partner institution, and that date will be recorded here when it is set.

IN PLAIN LANGUAGE

- Identity verification is mandatory before any disbursement, with no override.
- The licensed institution owns the AML obligation; Khepee provides the tooling and the evidence.
- Documents are encrypted, and every access is recorded with a stated purpose.
- Suspicious activity is escalated to the institution, which makes any regulatory report.

This summary is provided to aid understanding. It is not a substitute for the formal text, which governs.

> Khepee is a technology service provider operated by Lacspace Corporation Pvt. Ltd. It is not a bank or financial institution. It does not lend, does not accept deposits and does not hold customer funds. Lending products are provided by partner institutions licensed by Nepal Rastra Bank, and all credit decisions are theirs.

Contents

1 Scope and responsibility

1.1 Who owns the obligation
Anti-money-laundering and customer due diligence obligations rest with the licensed institution. Khepee is a technology provider and is not itself a reporting entity in respect of the lending.

1.2 What Khepee supplies
Verification workflow, encrypted document storage, duplicate detection, screening integration points, an append-only audit trail and reporting extracts.

1.3 What the institution supplies
Its risk appetite, its customer acceptance policy, its screening lists and providers, its reporting officer and its regulatory reporting.

1.4 Not legal advice
This document describes platform behaviour. It is not legal advice and does not replace the institution's own AML policy.

2 Customer identification

2.1 Mandatory before disbursement
No disbursement can occur without a verified identity. This is enforced structurally in the application state machine and cannot be overridden.

2.2 Accepted documents
Citizenship certificate, national identity card, passport, driving licence and voter identity card. The first three are treated as primary proof of identity.

2.3 Data captured
Document type, number, issuing district and date where applicable, and images of the relevant faces of the document.

2.4 Biometric check
A verification selfie and liveness check may be required, at the institution's configuration. The provider sits behind an interface and is chosen by the institution.

2.5 Human review
An automated result is advisory. A person at the institution records the verification decision.

2.6 Rejection requires a reason
A rejected verification cannot be saved without a written reason, which is retained.

2.7 Expiry and re-verification
Verifications carry an expiry. An application whose verification has lapsed returns to review rather than proceeding on stale evidence.

2.8 Duplicate detection
A deterministic keyed index over encrypted identifiers detects repeat applications within an institution without decrypting stored values.

3 Ongoing monitoring

3.1 Transaction records
Disbursements and repayments are recorded as immutable events with external references from the institution’s rails.

3.2 Pattern visibility
Repeat applications, rapid re-borrowing and unusual repayment patterns are surfaced to the institution for its assessment.

3.3 Screening integration
Sanctions and politically-exposed-person screening integrate through the same vendor-interface discipline as identity verification.

3.4 Escalation
Where the platform surfaces a concern, it is escalated to the institution. Khepee does not make a suspicion determination or file a report.

3.5 Institution reporting
Any suspicious transaction report or regulatory notification is made by the institution under its own obligations.

3.6 Tipping off
Platform personnel must not disclose to a borrower that a concern has been escalated.

4 Records and evidence

4.1 Retention period
Borrower records are retained for five years after loan closure, consistent with anti-money-laundering record-keeping expectations.

4.2 Immutable trail
Verification submissions, decisions, reasons and reviewers are written to an append-only record that cannot be edited or deleted.

4.3 Access is purpose-bound
Every access to verification data declares a purpose from a fixed list and is recorded with the person and time.

4.4 Encrypted storage
Document numbers and personal fields are encrypted at rest. Document images are stored as keys and served only through short-lived signed links.

4.5 Examiner access
Records can be produced for the institution and its regulator, filtered by borrower, period or officer.

4.6 Export discipline
Bulk export requires a distinct permission and a declared purpose, and is itself recorded.

5 Governance

5.1 Institution reporting officer
Each partner institution nominates the officer responsible for AML matters, and platform escalations are routed to them.

5.2 Configuration change control
Changes to verification requirements are configuration changes recorded in the audit trail with the person who made them.

5.3 Vendor approval
No verification or screening vendor is enabled without the institution's written selection. The platform ships with no real provider connected.

5.4 Training
Officer training covers the verification workflow, the reasons requirement and the escalation route.

5.5 Review
This document is reviewed at least annually and whenever a relevant directive changes.

5.6 Contact
aml@khepee.com for escalation of platform-level AML matters; compliance@khepee.com for regulatory correspondence.

Document control

Published by Lacspace Corporation Pvt. Ltd., Kathmandu, Nepal. Version 1.0, published 2026-07-30, last updated 2026-07-30. Status: Takes effect at launch. This document is published for review and does not yet bind anyone. It commences on the date the Khepee lending service goes live with a licensed partner institution, and that date will be recorded here when it is set. The authoritative version is published at khepee.com/legal/aml-kyc-policy and prevails over any printed or downloaded copy.

Khepee is a technology service provider operated by Lacspace Corporation Pvt. Ltd. It is not a bank or financial institution. It does not lend, does not accept deposits and does not hold customer funds. Lending products are provided by partner institutions licensed by Nepal Rastra Bank, and all credit decisions are theirs.

This document is published in English. Any translation is provided for convenience only; the English version governs in the event of inconsistency. This document is provided in good faith and does not constitute legal advice.