ONE VERIFY LTD

DATA RETENTION AND DISPOSAL POLICY

Effective Date: 1ST SEPTEMBER 2026

1. PURPOSE

This Policy establishes the principles governing the retention, archival, deletion, anonymisation and secure disposal of Personal Data and other information processed by One Verify.

2. SCOPE

This Policy applies to:

- Identity Data;
- Verification Data;
- Client Data;
- technical logs;
- API logs;
- account information;
- audit records;
- security records;
- contractual records; and
- other Personal Data processed by One Verify.

3. RETENTION PRINCIPLE

One Verify shall not retain Personal Data indefinitely.

Personal Data shall be retained only for the period reasonably necessary for:

- the purpose for which it was collected;
- contractual obligations;
- regulatory requirements;
- legal obligations;

- security;
- fraud prevention;
- audit;
- dispute resolution; or
- enforcement of legal rights.

4. IDENTITY VERIFICATION DATA

Identity verification information shall be retained only for the period required for the relevant verification purpose and applicable legal, regulatory and contractual obligations.

5. VERIFICATION RESULTS

Verification results may be retained for legitimate audit, compliance, dispute-resolution and contractual purposes, subject to applicable retention requirements.

6. NIMC-RELATED INFORMATION

NIMC-related information shall be retained, processed and disposed of in accordance with applicable NIMC requirements, the NIMC Act 2026, applicable regulations and contractual requirements governing access to NIMC services.

7. BIOMETRIC DATA

Where biometric information is processed, it shall be subject to enhanced access controls and shall not be retained beyond the period reasonably necessary for the lawful purpose for which it was collected, subject to applicable legal and regulatory requirements.

8. API AND SECURITY LOGS

Technical and security logs may be retained for purposes including:

- fraud prevention;
- security monitoring;

- incident investigation;
- troubleshooting;
- audit; and
- regulatory compliance.

9. LEGAL HOLD

Where information is required for litigation, investigation, regulatory review, audit or another legal process, deletion may be suspended until the relevant matter has been resolved.

10. DELETION AND DISPOSAL

When the applicable retention period expires, Personal Data shall be:

- securely deleted;
- irreversibly anonymised; or
- otherwise securely disposed of.

11. ACCESS CONTROL

Only authorised personnel shall have access to retained Personal Data.

Access shall be based on business need and appropriate role-based controls.

12. PERIODIC REVIEW

Retention periods shall be periodically reviewed to ensure that they remain appropriate and consistent with:

- applicable law;
- NIMC requirements;
- NDPA requirements;

- Client agreements;
- business requirements; and
- information-security requirements.

13. RESPONSIBILITY

The relevant compliance, privacy, legal, information-security and business teams shall be responsible for implementing and monitoring this Policy.