

Customer Due Diligence Policy

General customer verification, fraud prevention, and recordkeeping policy

Company	Morland NV
Company Registration No.	155703
Registered Address	Abraham de Veerstraat 9, Curaçao
Effective Date	July 2, 2026

1. Purpose

This policy describes how Morland NV verifies customer information, prevents fraud, maintains reliable records, and supports secure account administration for general digital services.

2. Scope

- Customers registering for company digital services.
- Business partners, vendors, or service providers where identity or ownership checks are appropriate.
- Transactions, support requests, or account changes that create elevated fraud, security, or compliance risk.

3. Customer Information

- Full legal name, date of birth where age verification is relevant, nationality or country of residence, and contact details.
- Residential or business address where needed for billing, account recovery, fraud prevention, or legal purposes.
- Payment-method ownership information where refunds, chargebacks, or fraud prevention require verification.

4. Verification Process

Step	Requirement
Standard Check	Verify identity and contact details using reliable documents or trusted third-party tools when necessary.
Address Check	Request a recent utility bill, bank statement, government correspondence, or other reliable address evidence when needed.
Payment Check	Confirm that the payment method belongs to the customer or authorized business representative.
Enhanced Check	Request source-of-funds, ownership, or additional documentation for high-risk or unusual account activity.

5. Risk-Based Review

- Low-risk customers may complete standard verification only.
- Higher-risk customers may require enhanced verification, senior review, additional monitoring, or account restrictions.
- Risk factors include inconsistent information, unusual activity, high-value transactions, adverse media, high-risk geography, or suspected misuse of services.

6. Ongoing Monitoring and Escalation

- Customer activity should be reviewed for fraud indicators, account takeover indicators, chargeback patterns, and unusual changes.
- Suspicious activity must be escalated to management or the appointed compliance contact.
- Decisions to restrict, suspend, or close an account must be documented with supporting reasons.

7. Records and Confidentiality

- Verification records must be stored securely with access limited to authorized personnel.
- Records should be retained only for the period required by business, legal, tax, audit, or dispute-resolution needs.
- Personal data must not be shared with third parties unless required for service delivery, fraud prevention, legal obligations, or customer authorization.

8. Contact

Questions about this policy may be directed to admin@feixinx.com.

9. Document Control

Version	Date	Owner	Summary
1.0	July 2, 2026	Compliance / Management	Neutralized from sector-specific KYC wording to general customer due diligence.

Approved by: Sandu Claudiu Gabriel_____

Name / Title: Director_____

Date: July 2, 2026 