

Information Security Policy

General corporate information-security framework

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

1. Purpose and Scope

This policy defines the baseline controls used to protect company information, customer data, business records, systems, and third-party integrations. It applies to employees, contractors, vendors, administrators, and any person with access to company systems.

2. Security Principles

- Confidentiality: information is accessed only by authorized persons with a business need.
- Integrity: systems and records are protected against unauthorized alteration.
- Availability: critical services are designed, monitored, and supported to maintain continuity.
- Accountability: access, approvals, changes, and incidents are logged and reviewed.

3. Data Protection and Encryption

- Sensitive records must be encrypted in transit using current TLS standards and at rest using strong encryption controls.
- Customer identity, contact, account, support, and transaction-related records must be stored only in approved systems.
- Data minimization must be applied: collect only what is needed for a legitimate business purpose.

4. Access Management

Control	Requirement
Least Privilege	Users receive only the access necessary for their approved role.
MFA	Multi-factor authentication is required for administrative, cloud, finance, and production access.
Joiner/Mover/Leaver	Access is granted, changed, and revoked through documented approval steps.
Access Review	Privileged access is reviewed at least quarterly.

5. Infrastructure and Vulnerability Management

- Development, staging, and production environments must remain logically separated.
- Security patches must be applied according to risk and operational impact.
- Independent or internal vulnerability testing should be performed periodically and after major platform changes.
- Backups must be protected, access-controlled, and tested for restoration.

6. Incident Response

- Suspected security incidents must be reported immediately to management or the appointed security contact.
- Incidents must be triaged, contained, investigated, remediated, and documented.
- Material incidents involving personal data must be escalated for legal and regulatory review before external notifications are made.

7. Vendor and Third-Party Security

- Vendors with access to company data or systems must be reviewed before onboarding.
- Contracts should include confidentiality, data protection, incident notification, and access-control obligations.
- Critical vendors should be reviewed at least annually or upon major service changes.

8. Document Control

Version	Date	Owner	Summary
1.0	July 2, 2026	Security / Management	Reformatted and neutralized for general corporate use.

Approved by: _____Sandu Claudiu Gabriel

Name / Title: _Director_____

Date: July 2, 2026

Sandiu