

OXILIUM N.V.

INFORMATION SECURITY POLICY (ISP)

Version: 2025.1

Jurisdiction: Curaçao

Document Classification: Internal / Regulatory Submission

1. Purpose & Regulatory Basis

This Information Security Policy (“Policy”) establishes the technical, organisational, architectural, and governance controls necessary to ensure the confidentiality, integrity, and availability of all information processed by Oxilium N.V. (“the Company”) and to satisfy Curaçao’s regulatory framework.

Security controls under this Policy follow a risk-based and proportionate approach, as required by the CGA Technical Standards and consistent with the Company’s overall risk profile and operational complexity.

This Policy supports compliance with:

- National Ordinance on the Identification of Natural Persons and Legal Entities (NOIS)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Sanctions National Ordinance (PB 2014 No. 55)
- Kingdom Sanction Act
- LOK - National Ordinance on Games of Chance
- CGA AML/CFT/CPF Regulations (2024-2025)
- CGA Technical Standards 11, 12, 13
- FIU Curaçao goAML reporting and technical requirements
- ISO/IEC 27001:2022 controls applied proportionately

This Policy forms a core component of Oxilium’s integrated compliance architecture and must be read together with:

- AML/CFT/CPF Policy (13 November 2025)
- KYC / CDD Policy (2025.1)
- Sanctions & Targeted Financial Sanctions Procedures
- Operational Manual

Where any conflict arises, Curaçao law and binding regulatory guidance prevail.

2. Scope

This Policy applies to:

- all Company systems, networks, databases, servers and cloud environments
- all AML/KYC/sanctions/monitoring platforms
- all customer personal, financial, behavioural and transactional data
- all employees, contractors, compliance officers and IT personnel
- all PSPs, data processors, hosting providers, and third-party vendors

- all information exchanged with FIU Curaçao, CGA, PSPs, banks and acquirers

Covers full data lifecycle: collection → transmission → processing → storage → access → backup → retention → destruction.

3. Information Security Objectives

3.1 Confidentiality

Regulated data (KYC/EDD, AML logs, sanctions files, CRA scoring, UTR/ISR data) must be:

- encrypted at rest (AES-256)
- encrypted in transit (TLS 1.2+)
- stored within authorised secure environments
- accessed strictly on a need-to-know basis

3.2 Integrity

The Company maintains controls ensuring that regulated data is:

- tamper-evident
- version-controlled
- validated via checksums or equivalent integrity mechanisms
- fully auditable

3.3 Availability

Critical systems must maintain:

- 24/7 availability
- $RTO \leq 24$ hours
- $RPO \leq 4$ hours

3.4 Accountability

All access or modification of regulated data must be:

- uniquely attributable
- logged and timestamped
- reviewable by Compliance, IT Security and Internal Audit

4. Definitions

- Regulated Data: all AML, KYC, EDD, sanctions, CRA, ISR/UTR and monitoring datasets.
- RDE (Regulated Data Environment): logically and/or physically segregated environment where regulated data is stored and processed.
- Security Incident: any event impacting confidentiality, integrity, availability or access control.
- Data Breach: unauthorised access, disclosure, alteration or exfiltration of regulated data.

5. Governance & Responsibilities

5.1 Board of Directors

Ensures:

- adequate resources for security
- independence of Compliance and IT Security
- approval of annual ISP updates
- timely remediation of vulnerabilities

5.2 CISO

Responsible for:

- implementing and maintaining all security controls
- vulnerability management and penetration testing
- access control architecture
- evaluating new technologies
- reporting material risks

5.3 AMLCO / MLRO

Responsible for:

- access governance for regulated data
- NORUT-compliant audit trails
- secure UTR submissions
- FIU/CGA breach notifications

5.4 IT Security

Handles:

- system hardening and patching
- SIEM monitoring and threat detection
- privileged access monitoring
- forensic support

5.5 All Employees

Must comply with this Policy, training requirements, credential security and incident reporting obligations.

6. Segregation of Duties (Mandatory CGA Control)

- IT/Developers: no access to regulated data; limited access may be granted to controlled non-production environments.
- Compliance: cannot modify infrastructure or production systems.
- Payments/Operations: cannot conduct CDD/EDD or risk scoring.
- Support: communication-only access, never verification.
- Administrators: cannot disable audit logging or monitoring.

Any violation is classified as a Security Incident.

7. Security Architecture

7.1 Segmented Network Zones

Zone 0 - Public Zone

Customer-facing interfaces.

Zone 1 - DMZ / Application Gateway

WAF

API gateway

DDoS mitigation

Zone 2 - Internal Operations Zone

Internal systems

Zone 3 - Regulated Data Environment (RDE)

Stores:

- KYC/EDD documents
- AML logs
- sanctions/TFS files
- CRA scoring
- UTR/ISR histories
- regulatory submissions

The RDE is logically and/or physically segregated from all other operational systems.

RDE access requires:

- MFA
- encrypted VPN
- device whitelist
- explicit approval (CISO + AMLCO)
- full audit logging

8. Access Control Framework

8.1 RBAC

- AMLCO/MLRO - full regulated data access
- KYC Officers - identity verification data only
- EDD Analysts - high-risk cases only
- Support - limited access
- Developers - no access to regulated data
- IT Admin - configuration-only access

8.2 Zero-Trust

- continuous authentication
- device integrity checks
- geo/IP risk evaluation
- anomaly-based session termination

8.3 Privileged Access Monitoring

All privileged actions must be logged, monitored and periodically reviewed.

9. Cryptography & Secure Data Handling

- AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- encrypted backups
- HSM/KMS key storage
- periodic key rotation and revocation
- hashing of metadata and credentials

10. Audit Logging (CGA TS11–13, NORUT)

Logs must include:

- access to regulated data
- CDD/EDD/CRA creation/modification
- sanctions screening hits and outcomes
- AML alert analysis
- UTR/ISR workflows
- FIU/CGA communications
- authentication failures
- privileged actions

Logs must be:

- append-only / tamper-evident
- time-synchronised (NTP)
- retained ≥ 5 years
- exportable for regulators

11. Sanctions & TFS Security Controls

Must include:

- onboarding and continuous sanctions screening
- freezing of assets without delay
- preservation of freeze files in RDE
- unfreezing only with AMLCO and regulator instruction
- full audit trail of actions

12. Monitoring & Threat Detection

SIEM and behavioural monitoring detect:

External threats

- DDoS
- credential stuffing
- exploitation attempts

Internal threats

- after-hours access
- mass file access
- unauthorised downloads
- privilege escalation attempts

Compliance-related anomalies

- prohibited-jurisdiction logins
- device fingerprint inconsistencies
- abnormal transaction patterns
- attempts to bypass controls

Monitoring incorporates typologies and indicators published by FIU Curaçao and relevant international bodies.

13. Incident Response Framework

Incident categories:

- security incident
- data breach
- insider misuse
- sanctions violation
- AML trigger event
- monitoring/logging integrity failure

Steps include:

1. Detection
2. Containment
3. Escalation
4. AMLCO review
5. Forensics
6. Root cause analysis
7. Remediation
8. Preventive actions
9. Documentation
10. Reporting to FIU/CGA where required

Breaches of segregation-of-duties automatically trigger this process.

14. Business Continuity & Disaster Recovery

Requirements:

- redundancy in CGA-approved jurisdictions
- encrypted daily backups
- offsite replication
- annual DR testing
- documented failover

Sanctions screening systems must be restored with the highest priority due to statutory freezing obligations.

Priority recovery sequence:

1. sanctions screening
2. AML monitoring
3. KYC verification
4. UTR submission infrastructure

15. Vendor & Third-Party Security

Vendors must:

- operate from FATF/EU-equivalent jurisdictions
- pass sanctions screening
- undergo onboarding and annual due diligence
- provide ISO27001/SOC2 or equivalent
- sign data protection / AML agreements
- provide annual penetration-test certification

Non-compliant vendors → remediation → suspension/termination.

16. Crypto Security Controls (If Enabled)

Crypto controls apply only if crypto functionality is activated in the business model.

Requirements:

- multi-signature wallets
- HSM/KMS key storage
- use of mixers, tumblers and privacy-enhanced cryptocurrencies is restricted and subject to AMLCO approval
- blockchain analytics proportionate to risk
- sanctions/darknet exposure screening
- AMLCO approval for high-value transfers

17. Data Retention & Secure Destruction

Retain ≥ 5 years:

- KYC/AML/EDD/CRA files

- sanctions decisions
- UTR/ISR files
- audit logs

Destruction follows NIST 800-88.

18. Training & Awareness

Annual mandatory training includes:

- security hygiene
- phishing/social engineering
- secure handling of identity documents
- AML/KYC/sanctions data protection
- incident reporting

All participation is logged.

19. Policy Review & Maintenance

This Policy is reviewed:

- annually
- upon regulatory updates
- upon updates to AML/KYC Policies
- after significant incidents or audit findings

Revisions require Board approval.