Anti-Money Laundering Policy Extract (Sample)

SAMPLE DOCUMENT — FOR TRAINING PURPOSES ONLY

This document is a synthetic sample created for the "Enjoy the Sun with AI" course. It does not represent real company data or policies.

1. Purpose

This policy establishes the framework for preventing money laundering, terrorist financing, and other financial crimes through our merchant services platform. It applies to all employees involved in merchant onboarding, monitoring, and compliance.

2. Customer Due Diligence (CDD)

Standard CDD must be completed for all new merchants before processing is enabled:

a) Verify identity of Ultimate Beneficial Owners (UBOs) holding >25% ownership
b) Verify registered business address and trading address
c) Screen against sanctions lists (OFSI, EU, UN)
d) Screen for Politically Exposed Persons (PEPs)
e) Verify source of funds for high-risk industries

CDD records must be retained for 5 years after the business relationship ends.

3. Enhanced Due Diligence (EDD)

EDD is required when:

a) The merchant operates in a high-risk industry (gambling, crypto, adult, travel)
b) The merchant's chargeback ratio exceeds 1.0% (Visa) or 1.5% (Mastercard)
c) ComplyAdvantage screening returns a CRITICAL or HIGH severity alert
d) Monthly processing volume exceeds £500,000
e) The merchant is domiciled in a high-risk jurisdiction

EDD includes: enhanced source of funds verification, senior management approval, ongoing transaction monitoring with reduced thresholds, and quarterly review cycle.

4. Ongoing Monitoring

All merchants are subject to ongoing monitoring:

Standard risk: Annual CDD refresh
Medium risk: Semi-annual CDD refresh + quarterly transaction review
High risk: Quarterly CDD refresh + monthly transaction review
Critical risk: Monthly CDD refresh + weekly transaction review

ComplyAdvantage alerts must be reviewed within:
CRITICAL: 4 hours
HIGH: 24 hours
MEDIUM: 72 hours

LOW: 5 business days

5. Suspicious Activity Reporting

If suspicious activity is identified, the compliance analyst must:

1. Document findings in the KYC Monitoring Portal (KMP)
2. Escalate to the MLRO within 24 hours
3. Do NOT inform the merchant (tipping off is a criminal offence)
4. The MLRO will determine whether a Suspicious Activity Report (SAR) is required
5. File SAR with the NCA via the SAR Online system if warranted
6. Maintain all records in KMP for audit trail