شركة شبكة الخدمات الآلية
Automated Services Network Co.

CODE OF CONDUCT & WHISTLEBLOWING POLICY

Version 1.7
Effective Date: [7/10/2026]

Document Title	Code of Conduct & Whistleblowing Policy
Version	1
Classification	Confidential — Internal & Regulatory Use
Review Cycle	Annual, or upon material regulatory/organizational change
Policy Owner	Compliance Department
Custodian	Human Resources & Internal Audit
Approving Authority	Board of Directors, following Audit Committee review
Related Documents	eNet-POL-FRD-001 Corporate Fraud Policy; AML/CFT Policy; Information Security Policy; HR Disciplinary Procedures
Regulatory Alignment	Central Bank of Kuwait (CBK) Instructions for MSPs; Kuwait AML/CFT Law No. 106 of 2013; ACFE Fraud Prevention Principles; ISO 31000; Kuwait Data Privacy Regulations; Kuwait Labour Law No. 6 of 2010

Contents

1. Purpose, Scope & Guiding Principles 3
1.1 Purpose 3
1.2 Scope of Application 3
1.3 Guiding Principles 3
2. Ethical Conduct 3
2.1 Conflict of Interest 3
2.2 Professional Conduct, Anti-Harassment & Inclusion 4
2.3 Confidentiality & Data Privacy 4
3. Regulatory Compliance & Fair Dealing 4
3.1 AML/CFT Commitment 4
3.2 Fair Dealing with Merchants & BNPL Customers 4
3.3 Anti-Bribery & Corruption 5
4. Asset & Operational Integrity 5
5. Speak-Up: Whistleblowing Framework 5
5.1 Duty to Report & Speak-Up Commitment 5
5.2 What May Be Reported 5
5.3 Reporting Channels 6
5.4 Confidentiality, Anonymity & Non-Retaliation 6
5.5 Case Handling & Investigation 7
5.6 External Reporting Obligations 7
6. Roles & Responsibilities 7
7. Accountability & Disciplinary Measures 8
8. Acknowledgment, Recordkeeping & Governance 8
8.1 Annual Acknowledgment 8
8.2 Case Register & Reporting to the Board 8
8.3 Ownership, Review & Communication 8

1. Purpose, Scope & Guiding Principles

"At eNet, integrity is not a compliance checkbox; it is our corporate identity. We operate at the center of Kuwait's digital payment ecosystem, entrusted daily with the funds, data, and confidence of our customers, merchants, and correspondent banking partners. That trust cannot be rebuilt once lost. Every employee, from the Board to the newest team member, is a Line of Defense for this ecosystem. Raising a concern in good faith is an act of loyalty to eNet, not disloyalty."

1.1 Purpose

This Code of Conduct & Whistleblowing Policy (the "Policy") sets out the standards of ethical behavior, professional conduct, and regulatory compliance expected of everyone acting on behalf of Automated Services Network Co. ("eNet", "the Company"), and the confidential, protected channel for raising concerns about wrongdoing.

1.2 Scope of Application

- All employees at every level, including Executive Management and the Board of Directors; contractors, consultants, secondees, and outsourced personnel; and vendors, merchants, agents, and third parties to the extent specified in their agreements.
- For whistleblowing (Section 5), also customers, members of the public, and former employees or contractors, in respect of matters arising during their engagement with eNet.

This Policy operates alongside eNet-POL-FRD-001, the AML/CFT Policy, the Information Security Policy, and HR Disciplinary Procedures.

1.3 Guiding Principles

Integrity: acting honestly, even when unobserved or under commercial pressure; **Accountability**: owning decisions and promptly disclosing conflicts, errors, or concerns; **Respect**: treating colleagues, customers, and partners fairly and without discrimination; **Stewardship**: safeguarding the funds, data, and infrastructure entrusted to eNet as one's own.

2. Ethical Conduct

2.1 Conflict of Interest

A Conflict of Interest arises when personal, financial, or familial interests could reasonably be perceived to compromise, or actually compromise, objectivity or loyalty. Any actual, potential, or perceived conflict must be promptly disclosed in writing to the Compliance Department, including:

- Financial interests in a merchant, vendor, correspondent bank, competitor, or business partner of eNet, and outside employment, consultancy, or directorships that may overlap eNet's business.
- Family or close personal relationships with an employee, vendor, merchant, or regulator's representative involved in decisions affecting that individual.
- Participation in hiring, procurement, onboarding, credit approval (including BNPL underwriting), or vendor selection involving a related party, and any gift or hospitality from a party doing business with eNet (Section 3.3).

Declarations are due on joining, when a conflict first arises, and annually (Section 8.1). Compliance may require recusal, reassignment, enhanced oversight, or restricted system access. Failure to disclose a known conflict is itself a breach.

2.2 Professional Conduct, Anti-Harassment & Inclusion

Employees must act professionally with colleagues, customers, merchants, banks, regulators, and the public, including on digital and social media attributable to eNet, and must not bring the Company into disrepute. Alcohol or any substance impairing judgment is prohibited. **eNet strictly prohibits harassment, bullying, victimization, or discrimination** on the basis of gender, nationality, religion, disability, age, marital status, or any other characteristic protected under Kuwaiti law.

- Harassment includes unwelcome verbal, physical, or visual conduct that creates an intimidating, hostile, or offensive environment, including comments, jokes, or advances of a sexual nature. Concerns may be raised with a line manager, Human Resources, or through Section 5, and will be investigated promptly, fairly, and confidentially.
- Recruitment, promotion, training, and compensation decisions shall be based on merit, competence, and performance, free from bias.

2.3 Confidentiality & Data Privacy

eNet handles sensitive payment card, account, Civil ID/KYC, e-Wallet, and BNPL credit data. All individuals within scope must:

- Access and process such data strictly on a need-to-know basis, for purposes directly related to their role, in line with the Information Security Policy and card scheme standards; not extract or retain it outside approved systems; and follow retention and disposal schedules.
- Not disclose confidential Company, customer, or merchant information externally (including to family and friends) except as required by law or a valid court/regulatory order, through the authorized channel.
- Report any suspected or actual unauthorized access, loss, or disclosure immediately to Information Security and Compliance, to enable containment and, where required, notification to (CBK).

Confidentiality obligations survive the end of employment or engagement.

3. Regulatory Compliance & Fair Dealing

3.1 AML/CFT Commitment

eNet maintains a **zero-tolerance commitment** to preventing the use of its Payment Gateway, Payment Links, e-Wallet, and BNPL products for money laundering, terrorist financing, or any other financial crime, in adherence to Kuwait AML/CFT Law No. 106 of 2013 and CBK instructions.

- Staff involved in onboarding, monitoring, or settlement must comply with the AML/CFT Policy, including CDD, EDD for high-risk relationships, and ongoing monitoring; AML/CFT training is mandatory on induction and periodically thereafter.
- Unusual activity inconsistent with a customer's profile, or indicative of layering, structuring, or other typologies, must be escalated promptly to Compliance. Employees must never help a customer or merchant evade AML/CFT controls, sanctions screening, or monitoring thresholds.
- Employees must not disclose that a Suspicious Transaction Report (STR) has been filed or is being considered ("tipping off"), which is a criminal offense under Kuwaiti law.

3.2 Fair Dealing with Merchants & BNPL Customers

- Merchant onboarding, pricing, and terms must be applied consistently on objective risk and commercial criteria, free from favoritism or undisclosed conflicts; fees, settlement timelines, and service terms must not be misrepresented; complaints must be handled promptly and fairly.

- BNPL assessments must use approved, objective underwriting criteria; BNPL terms (installments, fees, late-payment consequences) must be disclosed clearly and not misleadingly, consistent with responsible lending and CBK consumer protection expectations.
- Customers in financial difficulty must be treated fairly; requests for exceptional forbearance, waiver, or restructuring must be escalated, not resolved outside approved processes.

3.3 Anti-Bribery & Corruption

eNet strictly prohibits offering, giving, soliciting, or accepting any bribe, kickback, or improper benefit, directly or through a third party, including to or from government officials, regulators, bank personnel, merchants, vendors, or customers.

- **Gifts & hospitality:** only modest, occasional, transparent items of nominal value that cannot reasonably influence a business decision, disclosed to Compliance per the Gifts & Hospitality Register threshold. Cash or cash equivalents are never permitted; anything involving government officials or regulators requires prior written Compliance approval.
- **Facilitation payments & kickbacks:** facilitation payments, and referral fees or commissions outside formally approved and disclosed arrangements, are strictly prohibited. Staff must recuse themselves from any decision where a personal benefit has been offered or implied.

4. Asset & Operational Integrity

- **Systems:** use Company systems (Payment Gateway, Payment Links, e-Wallet, payment switch connectivity, etc.) only for authorized purposes and within approved access rights; never bypass security controls or share credentials; report any suspected vulnerability immediately to Information Security.
- **Funds:** handle Company, customer (e-Wallet/settlement), and merchant funds strictly within approved authorization limits, segregation-of-duties, and reconciliation procedures; never use them for personal purposes, even temporarily; document and process expenses and vendor payments through approved channels.
- **Payment switch integrity:** any act or omission that could compromise the availability, integrity, or confidentiality of the payment switch is a serious operational risk event; follow change management, testing, and business continuity protocols before modifying production systems.

5. Speak-Up: Whistleblowing Framework

5.1 Duty to Report & Speak-Up Commitment

All employees have an affirmative duty to report known or reasonably suspected breaches of this Policy; failure to do so may itself be a breach subject to disciplinary action. Every report will be taken seriously, handled with discretion, and investigated objectively, and those who report in good faith are protected as set out below.

5.2 What May Be Reported

A "Protected Disclosure" is any good-faith report of a reasonable belief that misconduct, wrongdoing, or a material risk has occurred, is occurring, or is likely to occur, including (illustrative, not exhaustive):

Category	Illustrative Examples
Fraud & Financial Crime	Embezzlement, asset misappropriation, financial statement manipulation, payment or BNPL credit fraud (per eNet-POL-FRD-001).

Category	Illustrative Examples
AML/CFT Violations	Suspected money laundering, terrorist financing, sanctions evasion, failure to escalate suspicious activity, or tipping off.
Bribery, Corruption & Code Breaches	Bribes, kickbacks, improper gifts; undisclosed conflicts of interest; harassment or discrimination; misuse of confidential data.
Regulatory Non-Compliance	Failure to comply with CBK instructions, card scheme rules, other laws, or licensing conditions.
Data Privacy & Information Security	Unauthorized access to or disclosure of customer data, or concealment of a data breach.
Operational & Other Serious Misconduct	Concealed system failures, unauthorized production changes, acts compromising the payment infrastructure, health and safety risks, or any other serious ethical breach.

Purely personal workplace grievances with no ethical, legal, or regulatory dimension are better addressed through HR grievance channels; HR will redirect such matters if raised here in good faith. "Good faith" means an honest and reasonable belief in the truth of the information at the time of reporting, whether or not later substantiated; a report made knowing it is false, recklessly, or for an improper purpose is malicious.

5.3 Reporting Channels

Reports may be made through any of the following channels, at the reporter's discretion:

- **Whistleblowing Hotline/Mailbox:** a dedicated, confidential channel administered by Compliance, open to employees and external parties, supporting both identified and anonymous reports.
- **Line Manager or Department Head** (where not involved); **Compliance or Head of Internal Audit** (compliance, fraud, or audit matters); **Human Resources** (conduct, harassment, discrimination).
- **Audit Committee Chairman:** where the matter implicates Executive or Senior Management, or the reporter believes another channel would compromise confidentiality or create a conflict of interest. The Chairman determines independent handling, which may include external counsel or forensic investigators.

Reporters are encouraged, but not required, to include a description of the concern, relevant dates and references, and any supporting evidence. A report will not be deprioritized because it is incomplete or informally worded.

5.4 Confidentiality, Anonymity & Non-Retaliation

- **Confidentiality:** a whistleblower's identity is shared only with those directly assessing or investigating the report, and beyond that only where required by law, regulation, or a court/regulatory order, or to give the subject a fair opportunity to respond under eNet-POL-FRD-001 Section 6.4 — with advance notice to the whistleblower where practicable.
- **Anonymity:** anonymous reports are accepted and investigated to the extent the information permits; anonymity may limit follow-up and feedback.

eNet strictly prohibits any retaliation, intimidation, harassment, or adverse employment or contractual action against anyone who reports in good faith or cooperates with an investigation. Retaliation is itself a serious disciplinary matter, up to and including termination, regardless of the outcome of the original report.

- Protection applies whether or not the concern is substantiated, provided the report was made in good faith. Suspected retaliation should be reported immediately to Compliance or the Audit Committee Chairman and is treated as a priority; line managers are accountable for preventing direct or subtle adverse treatment of a known or suspected whistleblower.

- **Limits:** protection does not extend to knowingly false, malicious, or frivolous reports, or to those complicit in the wrongdoing reported. This is applied narrowly, after a fair assessment, so as not to discourage good-faith reporting.

5.5 Case Handling & Investigation

- **Intake & triage:** Compliance (or the Audit Committee Chairman, where applicable) logs each report in the Whistleblowing Case Register with a unique reference and assesses credibility, materiality, urgency, and category, taking conflicts of interest into account.
- **Case ownership:** fraud and financial crime — Internal Audit under eNet-POL-FRD-001 Section 6; Code of Conduct breaches — Human Resources with Compliance; AML/CFT matters — Compliance, including assessment of STR obligations to the Kuwait FIU; matters implicating Senior Management — the Audit Committee, which may engage independent investigators.
- **Timelines:** acknowledgment within five (3) business days of logging (where contact details exist); triage outcome within fifteen (15) business days of acknowledgment, subject to complexity; status updates and the outcome shared where feasible without compromising confidentiality or the investigation.
- **Interim measures & closure:** where necessary, interim measures (e.g., precautionary suspension of system access, temporary reassignment) may be applied consistent with eNet-POL-FRD-001 Section 6.3. Each case closes with a summary of findings, actions, and recommended remediation.

5.6 External Reporting Obligations

Certain reports trigger obligations independent of the internal process: material fraud, control failures, or misconduct is escalated to the **CBK**; indications of money laundering or terrorist financing are assessed by Compliance and, where warranted, reported to the **Kuwait FIU** by STR; criminal conduct is referred to the competent authorities with Legal Counsel; and card schemes and correspondent banks are notified where payment or settlement integrity is affected. A whistleblower is never identified in an external notification unless required by law or the authority's legal process.

6. Roles & Responsibilities

Role	Key Responsibilities
Board / Audit Committee	Approves this Policy; oversees the whistleblowing framework and receives periodic case reporting; oversees matters implicating Senior Management.
Compliance (Policy Owner)	Administers this Policy and the hotline/mailbox; assesses conflict declarations; performs intake and triage; leads AML/CFT matters and STR assessment; maintains the Case Register.
Internal Audit	Leads fraud-related investigations per eNet-POL-FRD-001; independently assesses the framework's effectiveness; verifies closure of remediation actions.
Human Resources	Administers the Annual Acknowledgment; leads conduct, harassment, and discrimination cases; administers discipline, including for proven retaliation.
Line Management	Models these standards; fosters a Speak-Up culture; never retaliates; escalates informally raised concerns through formal channels.
All Employees & Third Parties	Comply with this Policy; report suspected wrongdoing via Section 5; cooperate honestly with investigations; never retaliate against a reporter.

7. Accountability & Disciplinary Measures

This Policy is enforceable and applied consistently irrespective of seniority. Breaches are addressed through eNet's disciplinary framework, proportionate to severity, intent, and impact:

- Counseling or a formal written warning for minor or repeated lesser breaches; suspension pending investigation in line with Kuwaiti labour law and HR procedures.
- Termination for cause for serious breaches, including fraud, bribery, harassment, discrimination, AML/CFT violations, serious data privacy breaches, or retaliation against a whistleblower, following due process.
- Referral to law enforcement where conduct is a criminal offense; civil action to recover losses; and regulatory notification to the CBK and, where relevant, card scheme partners or correspondent banks.

Breaches involving fraud, embezzlement, or financial crime are investigated and sanctioned under eNet-POL-FRD-001, which governs investigation procedures, evidentiary standards, and the full range of consequences.

8. Acknowledgment, Recordkeeping & Governance

8.1 Annual Acknowledgment

All employees must confirm in writing (including electronically) that they have read, understood, and will comply with the current version of this Policy, together with a refreshed Annual Conflict-of-Interest Declaration (Section 2.1). Human Resources administers the process with Compliance, tracks completion, reports to Executive Management and periodically to the Audit Committee.

8.2 Case Register & Reporting to the Board

Compliance maintains a centralized, access-restricted Whistleblowing Case Register recording, for each report: date, channel, category, whether anonymous, investigation owner, milestones, outcome, and resulting disciplinary, control, or regulatory action. At least quarterly, Compliance reports to the Audit Committee, in aggregated and anonymized form, on reports received by channel and category, outcomes, average time to acknowledgment/triage/closure, material findings and systemic control weaknesses, and any suspected retaliation. Whistleblower identities are not disclosed except where a case requires the Committee's direct oversight under Section 5.3.

8.3 Ownership, Review & Communication

This Policy is owned by Compliance, with Human Resources and Internal Audit as co-custodians. It is reviewed at least annually, or sooner upon material regulatory change, restructuring, a significant conduct incident, or a whistleblowing case revealing a framework gap. Material amendments require review by the Audit Committee and Board approval before issuance. The Policy is communicated to all employees, contractors, and relevant third parties on issuance and at each revision, and reinforced through induction training and awareness campaigns.

Approval

Prepared By	Reviewed By	Approved By	
Compliance Department	Human Resources / Internal Audit	General Manager	Board of Directors (via Audit Committee)
Signature:	Signature:	Signature:	Signature: