Polices and produres File location 6.3.1

Third Party Risk Management Policy

Date: 10/8/2026

Ver. 1.5

Approved BY:

Sabah K. Al Ghunaim
Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

1. Purpose 3
2. Scope 3
3. Definitions 3
4. Regulatory and Standards Alignment 3
5. Governance and Responsibilities 4
   5.1 Board of Directors 4
   5.2 Senior Management 4
   5.3 Risk and Compliance Function 4
   5.4 Business Owners 4
6. Third-Party Risk Classification 4
7. Due Diligence and Onboarding 4
8. Contractual Requirements 5
9. Ongoing Monitoring and Review 5
10. Incident Management 5
11. Concentration and Dependency Risk 5
12. Exit Strategy and Business Continuity 6
13. Record Keeping and Reporting 6
14. Related Party Transactions 6
   14.1 Purpose 6
   14.2 Definition of Related Party 6
   14.3 Identification 7
   14.4 Governance and Approval 7
   14.5 Arm's-Length Pricing 7
   14.6 Related Party Register 7
   14.7 Monitoring and Disclosure 8
   14.8 Financial Responsibility for Secondment Arrangements 8
15. Policy Review 8
16. Approval 8

1. Purpose

This Third-Party Risk Management (TPRM) Policy establishes the governance framework through which Automated Services Network Company - eNet, as a licensed Large E-Money Service Provider (LESP), identifies, assesses, manages, monitors, and exits risks arising from its relationships with third parties. The objective is to ensure that outsourcing and third-party arrangements do not compromise financial stability, customer protection, data confidentiality, regulatory compliance, or operational resilience.

This Policy is designed to align with the expectations of the Central Bank of Kuwait (CBK) and applicable international best practices.

2. Scope

This Policy applies to:

- All third parties engaged by eNet, whether domestic or international
- All stages of the third-party lifecycle (onboarding, operation, renewal, and exit)
- All business units, subsidiaries, and functions of eNet

This Policy covers both contractual and non-contractual arrangements where services are provided to, or on behalf of, eNet.

3. Definitions

Third Party: Any external entity that provides services, technology, infrastructure, data processing, or operational support to eNet.

Critical Third Party: A third party whose failure or disruption could materially impact payment services, customer funds, regulatory compliance, data security, or eNet's ability to operate.

Outsourcing: An arrangement whereby a third party performs a process, service, or activity that would otherwise be undertaken by eNet.

Related Party: See Section 14.2 for the full definition applied under this Policy.

4. Regulatory and Standards Alignment

This Policy aligns with, but is not limited to:

- Central Bank of Kuwait regulations and supervisory guidance
- Operational Resilience principles
- PCI DSS requirements
- - ISO/IEC 27001, ISO 22301, ISO 31000
- Applicable data protection laws

5. Governance and Responsibilities

5.1 Board of Directors

- Approves this Policy and any material amendments
- Oversees third-party risk exposure and concentration risk
- Ensures adequate resources are allocated for effective implementation

5.2 Senior Management

- Implements the Policy across the organization
- Ensures compliance with regulatory requirements
- Escalates material third-party risks to the Board

5.3 Risk and Compliance Function

- Maintains the third-party risk framework
- Conducts risk assessments and due diligence
- Monitors ongoing compliance and performance

5.4 Business Owners

- Identify third-party dependencies
- Ensure services are delivered in line with contractual obligations
- Report incidents and performance issues

6. Third-Party Risk Classification

All third parties shall be classified based on risk and criticality:

Category	Description
Critical	Direct impact on payments, customer funds, core systems, or regulatory compliance
High	Access to sensitive data or production systems
Medium	Operational support with limited system or data access
Low	No access to sensitive data or critical systems

Risk classification determines the level of due diligence, monitoring, and approval required.

7. Due Diligence and Onboarding

Prior to engagement, eNet shall perform proportionate due diligence, including:

- Financial viability assessment
- Regulatory and licensing review (where applicable)
- Information security and data protection controls
- Business continuity and disaster recovery capabilities
- Sub-outsourcing arrangements

Evidence may include certifications, audit reports, policies, and independent assessments.

Critical and High-risk third parties require formal risk approval before onboarding.

8. Contractual Requirements

All third-party contracts must include, as applicable:

- Defined scope of services and SLAs
- Confidentiality and data protection obligations
- Incident and breach notification timelines
- Right of audit and regulatory access
- Business continuity and disaster recovery obligations
- Restrictions on sub-contracting
- Termination and exit provisions

Contracts with Critical Third Parties must be reviewed by **Legal and Compliance** functions.

9. Ongoing Monitoring and Review

ENet shall monitor third parties throughout the engagement lifecycle, including:

- Periodic performance and SLA reviews
- Annual risk reassessments for Critical and High-risk vendors
- Review of security posture and compliance status
- Tracking of incidents, breaches, and remediation actions

Monitoring frequency is risk-based.

10. Incident Management

Third parties must notify eNet of any incident that may impact services, data, or customers within agreed timelines.

ENet shall:

- Assess impact and regulatory notification requirements
- Coordinate response and remediation
- Document and report incidents internally and to regulators where required

11. Concentration and Dependency Risk

ENet shall identify and manage concentration risk arising from:

- Over-reliance on a single third party
- Geographical or systemic dependencies

Mitigation measures may include alternative providers, contingency plans, or contractual safeguards.

12. Exit Strategy and Business Continuity

For Critical Third Parties, documented exit plans must be maintained, including:

- Data return or secure destruction
- Knowledge transfer and transition support
- Continuity of service during migration

Exit strategies shall be tested periodically where feasible.

13. Record Keeping and Reporting

ENet shall maintain:

- An inventory of all third parties
- Risk assessments and due diligence records
- Contracts and amendments
- Monitoring and incident reports
- The Related Party Register maintained under Section 14

Records shall be made available to the Central Bank of Kuwait upon request.

14. Related Party Transactions

This section governs eNet's relationships with related parties, distinct from the general third-party framework. It addresses conflict-of-interest and arm's-length pricing risk arising from ownership, control, or personal relationships, risks that ordinary vendor due diligence does not test for. Related Party status adds a governance layer, not a substitute for the general third-party framework. Where a related party also is classified as a Critical or High third party under Section 6 (for example, based on the nature of services it performs or its access to systems, data, or customer funds), the corresponding due diligence, contractual, and monitoring requirements under Sections 6–9 continue to apply in full, alongside, not instead of, the requirements of this Section.

14.1 Purpose

To ensure that all transactions and arrangements between eNet and its related parties are identified, independently reviewed, approved on arm's-length terms, monitored, and disclosed in accordance with CBK expectations.

14.2 Definition of Related Party

A Related Party includes, without limitation:

- Any entity under common ownership or control with eNet (e.g., eNet Integrated Solutions Co.)
- Members of the Board of Directors and Senior Management, and their close family members
- Any entity in which a Director or member of Senior Management holds a significant ownership interest or exercises significant influence
- Any other party classified as related under applicable CBK regulation

14.3 Identification

- Directors and Senior Management shall submit an annual Declaration of Interests disclosing affiliations that may constitute a related party relationship, and shall update this declaration promptly upon any change.
- The Risk and Compliance Function shall maintain the criteria above and proactively flag subsidiaries, affiliates, and known related individuals for inclusion in the Related Party Register (Section 14.6).

14.4 Governance and Approval

- Any transaction or arrangement with a Related Party requires independent review by the Risk/Audit Committee prior to approval, irrespective of the value or nature of the arrangement.
- Any Director or member of Senior Management with a personal interest in a proposed related party transaction shall declare that interest and recuse themselves from its discussion, review, and approval.
- No related party transaction shall be approved on the sole authority of the individuals representing both sides of the arrangement.

14.5 Arm's-Length Pricing

- All related party transactions shall be conducted on arm's-length terms, reflecting the pricing and conditions that would apply between unrelated parties in a comparable transaction.
- Where a direct market benchmark is unavailable, a documented cost-plus or comparable pricing methodology shall be applied and retained as supporting evidence for the Risk/Audit Committee's review.

14.6 Related Party Register

The Compliance Function shall establish and maintain a centralized Related Party Register recording, at minimum:

- Identity of the related party and nature of the relationship
- Nature and value of transactions or arrangements with the related party
- Approval reference (Risk/Audit Committee review date; Board resolution reference where applicable)
- Date of last review and next scheduled re-certification

The Register shall be reviewed and re-certified at least annually, and cross-referenced with the records maintained under Section 13.

14.7 Monitoring and Disclosure

- Related party relationships and transaction terms shall be re-certified annually, or immediately upon any material change in ownership, control, or personnel.
- Related party transactions shall be disclosed in eNet's financial statements and reported to the Central Bank of Kuwait where required under applicable regulation.
- The Register and supporting approval records shall be made available to the Central Bank of Kuwait and external auditors upon request.

14.8 Financial Responsibility for Secondment Arrangements

- The Home Entity remains the employer of record for the seconded employee throughout the secondment. It is responsible for payment of the employee's salary and statutory entitlements, consistent with Section 3 of the applicable Secondment Agreement.

- The Host Entity reimburses the Home Entity for the value of the seconded employee's services through a documented cost allocation / cross-charge, applying the arm's-length pricing principles set out in Section 14.5.

- The specific cost allocation methodology for each secondment shall be recorded in the "Cost Allocation Reference" field of the individual Secondment Letter, and shall not be left blank.

- Where an employee performs duties spanning both entities without a documented secondment (e.g., an individual settling transactions or handling complaints for both eNet and a related party without a Secondment Letter identifying their role), this is treated as an unregularized related-party arrangement requiring immediate documentation under this Section, and is escalated to the Risk and Compliance Function for corrective action.

15. Policy Review

This Policy shall be reviewed at least annually or upon material regulatory or business changes.

16. Approval

This Policy is approved by the Board of Directors and is effective from the date of approval.

Position	Name	Signature
Chairman	Sabah K. Al Ghunaim	
Board Member 1	Lamiaa Khaled Al Kharafi	
Board Member 2	Khaled Sabah Al Ghunaim	
General Manager	Jamal Kubeer	
Sales Manager	Afif Moukahel	
Administration Manager	Nesrine Zakaria	
Finance Manager	Abdul Rahman El Rotel	
Risk Department	El Sayed Thabet	