Operational Resilience Policy

eNet Automated Services Network Company (EMSP)

v1

Date: 11-1-2026

Approved by

Sabah K. Al Ghunaim

Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

1. Purpose

This policy establishes eNet's operational resilience framework to ensure uninterrupted delivery of e-money services, protect customer funds, and maintain trust in digital financial transactions. It aligns with regulatory requirements for Electronic Money Services Providers (EMSP) and international best practices in financial resilience.

2. Scope

- Applies to all eNet EMSP operations, including digital wallets, payment processing, settlement systems, and customer support.
- Covers IT infrastructure, transaction platforms, data centers, and third-party payment gateways.
- Extends to employees, contractors, agents, and outsourced service providers if any.

3. Policy Statement

eNet commits to:

- Safeguarding customer funds and transaction integrity.
- Ensuring continuity of critical payment and settlement services.
- Meeting regulatory obligations under financial authorities and central bank directives.
- Embedding resilience into technology, people, and processes.
- Rapid recovery from disruptions with minimal impact on customers.

4. Governance

- Board of Directors: Approves resilience strategy and ensures compliance with financial regulations.
- Risk & Compliance Officers: Oversees resilience planning, regulatory reporting, and risk management.
- Operational Coordination: Across IT, Finance, Compliance, and Customer Service.
- Employees & Agents: Must follow resilience protocols and report incidents immediately.

5. Key Principles for EMSP

- Critical Service Identification: Prioritize transaction processing, wallet access, settlement, and customer support.
- Cyber Resilience: Protect against fraud, hacking, and data breaches with layered security controls.
- Financial Resilience: Maintain liquidity buffers and contingency funding to ensure uninterrupted settlement.
- Business Continuity & Disaster Recovery: Maintain tested recovery plans for payment systems and customer data.
- Regulatory Compliance: Align with Central Bank of Kuwait (or relevant authority) and AML/CFT/WMD (Anti-Money Laundering/Counter-Terrorist Financing/Ani-Prefiltration of Weapons of Mass Destruction) requirements.
- Third-Party Oversight: Ensure payment processors, and agents meet resilience standards.
- Customer Protection: Guarantee transparent communication and rapid resolution during service disruptions.

6. Resilience Framework

- Prevent: Fraud detection, cybersecurity monitoring, and vendor risk assessments.
- Prepare: Scenario testing (e.g., cyberattack, system outage, liquidity crisis).
- Respond: Crisis management team activation, regulatory notifications, and customer communication.
- Recover: Restore transaction services within defined Recovery Time Objectives (RTOs).
- Adapt: Post-incident reviews and policy updates.

7. Roles & Responsibilities

- Risk & Compliance Officers: Lead resilience compliance and regulatory engagement.
- IT & Security Teams: Ensure system uptime, fraud monitoring, and cyber defense.
- Finance Team: Maintain liquidity and settlement continuity.
- Customer Service: Provide transparent updates to customers during disruptions.
- Compliance Team: Ensure AML/CFT/WMD and regulatory reporting obligations are met.

8. Compliance & Standards

eNet EMSP aligns with:

- Business Continuity Management
- Information Security
- PCI DSS (Payment Card Industry Data Security Standard)
- AML/CFT/WMD Regulations (Central Bank regulations)
- Local e-Money Regulations governing EMSPs

9. Monitoring & Reporting

- Real-time monitoring of transaction systems and fraud detection.
- Daily liquidity and settlement checks.
- Incident reporting to regulators within mandated timelines.
- Resilience testing and Board reporting.

10. Recovery Objectives

To ensure continuity of e-money services, eNet defines clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical functions:

Critical Service	RTO (Max Downtime)	RPO (Max Data Loss)	Notes
Digital Wallet Access	2 hours	15 minutes	Customers must regain access quickly to avoid disruption in daily transactions.
Transaction Processing (Payments, Transfers)	1 hour	Near-zero (≤ 5 minutes)	Payment continuity is essential; data integrity must be preserved.
Settlement & Clearing Systems	24 hours	1 hour	Liquidity and settlement continuity must be maintained to meet regulatory obligations.
Customer Support Channels	4 hours	N/A	Alternative communication

			channels (IVR, email, social media) must be activated if primary systems fail.
Fraud Detection & Monitoring	1 hour	Near-zero (≤ 5 minutes)	Continuous fraud monitoring is critical to protect customer funds.
Regulatory Reporting Systems	24 hours	1 hour	Compliance reporting must resume within regulatory timelines.

11. Testing & Assurance

- RTOs and RPOs will be validated through annual resilience testing (including cyberattack simulations, system outages, and liquidity stress tests).
- Results will be reported to the Board of Directors and shared with regulators where required.
- Any gaps identified will trigger immediate remediation plans.

12. Continuous Improvement

- Post-incident reviews will assess whether RTOs and RPOs were met.
- Targets will be updated annually to reflect changes in technology, customer expectations, and regulatory requirements.

13. Regulatory Alignment of Recovery Objectives

eNet's Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are mapped to key regulatory and industry standards to ensure compliance and customer protection:

Critical Service	RTO / RPO	Regulatory / Standard Alignment	Compliance Notes
Digital Wallet Access	RTO: 2 hrs / RPO: 15 min	Central Bank of Kuwait EMSP Directive – customer access continuity;	Wallet downtime beyond 2 hrs may breach customer protection obligations.

Transaction Processing (Payments, Transfers)	RTO: 1 hr / RPO: ≤ 5 min	PCI DSS – transaction integrity; data security; AML/CFT/WMD Regulations	Near-zero data loss required to prevent fraud and AML breaches.
Settlement & Clearing Systems	RTO: 24 hrs / RPO: 1 hr	Central Bank of Kuwait Settlement Rules; Basel Committee Principles for Financial Market Infrastructures (PFMI)	Liquidity and settlement continuity must meet regulatory timelines.
Customer Support Channels	RTO: 4 hrs	Consumer Protection Regulations	Alternative channels must be activated to maintain customer communication.
Fraud Detection & Monitoring	RTO: 1 hr / RPO: ≤ 5 min	AML/CFT/WMD Directives; PCI DSS	Continuous monitoring is required to detect suspicious activity in real time.
Regulatory Reporting Systems	RTO: 24 hrs / RPO: 1 hr	Central Bank of Kuwait Reporting Requirements; AML/CFT/WMD Compliance	Reports must be filed within mandated timelines to avoid penalties.

14. Reporting Notification Protocol

- **Incident reports** submitted within 24 hours, including root cause analysis and recovery actions.

15. Audit Review & Assurance

- Annual **audit** of resilience measures.
- Documentation of all resilience tests retained for **inspection**.

16. Policy Review

This policy will be reviewed annually, or following:

- Regulatory changes in EMSP requirements.
- Significant incidents (e.g., cyberattack, payment outage).
- Organizational restructuring or new product launches.