DISASTER RECOVERY POLICY

NexaBank Digital

Document Ref: NBD-DR-POL-001 | Version: 2.2 | Classification: CONFIDENTIAL

Version Control

Version	Date	Author	Description	Status
1.0	12 Mar 2019	J. Osei (IT Director)	Initial DR Policy.	Approved
2.0	08 Jul 2021	J. Osei (IT Director)	Major revision. Added tiering framework. Updated FFIEC references.	Approved
2.1	14 Feb 2022	J. Osei (IT Director)	Added SWIFT recovery requirements.	Approved
2.2	20 Oct 2022	J. Osei (IT Director)	Quarterly replication monitoring added. Runbook standards updated.	Approved

Approval and Sign-Off

Role	Name	Signature	Date
Chief Technology Officer	A. Mensah	_____	20 Oct 2022
IT Director	J. Osei	_____	20 Oct 2022
Chief Risk Officer	B. Amponsah	_____	20 Oct 2022
Board Audit Committee (Chair)		_____	
Chief Compliance Officer		_____	
Head of Operations	E. Darko	_____	20 Oct 2022

GAPS: (1) Board Audit Committee sign-off is absent. FFIEC BCP Booklet requires board-level awareness and approval of DR policy. (2) Chief Compliance Officer sign-off is absent. For a FFIEC-regulated institution, compliance review of the DR policy is a regulatory expectation, not optional.

1. Purpose

This policy establishes NexaBank Digital's ("NexaBank" or "the Bank") framework for Disaster Recovery (DR) — the IT-specific capability to restore technology systems and services following a disruption event. NexaBank operates as a regulated financial institution under the Financial Institutions Examination Council (FFIEC) BCP Booklet requirements and must demonstrate robust DR capability to satisfy regulatory expectations. This policy is distinct from and complementary to the Business Continuity Plan.

2. Scope

This policy applies to all IT systems within NexaBank's declared DR scope, comprising 14 systems as documented in the System RTO/RPO Register (Annex A). In-scope systems include:

- Core Banking System (NexaCore v8.3)
- SWIFT messaging platform (Alliance Access)
- Internet Banking platform (NexaWeb)
- Payment processing engine (PayRoute)
- ATM network management system
- Card management system
- AML/fraud monitoring platform
- Supporting infrastructure: databases, middleware, network

AUDIT NOTE — DELIBERATE GAP

SCOPE GAP: This policy references 14 systems in Annex A, but Annex A is not included in this document. The replication failure event 8 months ago ran undetected for 8 days — suggesting that monitoring controls for in-scope systems may be insufficient. Systems added since the last policy review may not have formally declared RTO/RPO targets.

3. Recovery Objectives Framework

Each in-scope system must have documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) agreed between IT and the relevant business unit owner, formally approved by the IT Director.

Tier	Label	RTO Target	RPO Target	Examples	Review Frequency
1	Gold	< 1 hour	< 15 minutes	Core Banking, SWIFT, Payment Engine	Quarterly
2	Silver	< 4 hours	< 1 hour	Internet Banking, ATM Network, Card Mgmt	Semi-annual
3	Bronze	< 24 hours	< 4 hours	AML Platform, HR Systems, Reporting	Annual

AUDIT NOTE — DELIBERATE GAP

RTO/RPO GAPS: (1) RTOs must be validated against business-declared Maximum Tolerable Downtime (MTD). If RTO >= MTD, the business will breach its operational tolerance before recovery completes — this is a fundamental DR design failure. (2) No Board or senior management approval of RTO/RPO targets is required by this policy. FFIEC expects board awareness of recovery capability commitments. (3) IT-declared RTOs may not reflect realistic recovery times under actual disaster conditions — test results should validate declared RTOs, but test failures do not automatically trigger RTO revision.

4. Disaster Recovery Testing

4.1 Test Frequency

DR tests must be conducted at least annually for all in-scope systems. Tests must include participation from IT operations and the relevant business unit representatives.

> **AUDIT NOTE — DELIBERATE GAP**
> *TEST FREQUENCY GAP: Annual DR testing is the FFIEC minimum. For Gold-tier (critical) systems at a regulated bank, semi-annual testing is industry best practice. The last DR test was 14 months ago — this Bank is already overdue on its annual testing obligation. Tabletop exercises may be used to satisfy this requirement, meaning full failover may not have been tested in multiple years.*

4.2 Test Scope and Validation

DR tests must validate that RTO and RPO targets can be achieved under simulated disaster conditions. Tests must include restoration of data from backup to confirm data integrity in addition to system failover.

> **AUDIT NOTE — DELIBERATE GAP**
> *TEST SCOPE GAPS: (1) This policy does not require all 14 in-scope systems to be tested in each exercise — partial tests covering a subset of systems may be declared complete. (2) No requirement for independent validation of test results — IT may declare a test successful with no external verification. (3) Test results showing RTO overruns do not automatically require RTO revision or escalation to the board.*

4.3 Test Documentation and Remediation

Results of all DR tests must be documented including: systems tested, RTO achieved vs target, issues identified, action items with owners and due dates. Action items must be tracked to closure before the next DR test.

> **AUDIT NOTE — DELIBERATE GAP**
> *REMEDIATION GAPS: (1) "Tracked to closure before the next DR test" is stated but not enforced. No mechanism exists to prevent a test from being signed off with open high-severity action items. (2) FFIEC requires board reporting of DR test results — this policy does not require the IT Director to report test results to the board or audit committee.*

5. Recovery Runbooks

A recovery runbook must exist for each Tier 1 (Gold) system. Runbooks are recommended for Tier 2 (Silver) systems. Runbooks must contain step-by-step recovery procedures sufficient to enable execution by an IT professional unfamiliar with the system.

> **AUDIT NOTE — DELIBERATE GAP**
> *RUNBOOK GAPS — CRITICAL: (1) Runbooks are MANDATORY for Gold systems but only RECOMMENDED for Silver systems — a 4-hour RTO without a mandatory runbook is a significant operational risk. (2) No minimum content standard is defined for runbooks. (3) No version control requirement — runbooks may reference outdated system configurations, IP addresses, or credentials. (4) No requirement to update runbooks when system changes occur. (5) No requirement to test runbooks during DR exercises — a runbook may exist but have never been executed.*

6. Data Replication

Gold-tier systems must maintain real-time or near-real-time data replication to the secondary DR site. Replication health must be monitored daily by IT Operations. Silver-tier systems require minimum daily backup replication.

AUDIT NOTE — DELIBERATE GAP

REPLICATION GAPS: (1) No definition of "near-real-time" — acceptable replication lag is not quantified. A system replicating data every 4 hours may satisfy this requirement despite having a 15-minute RPO. (2) No escalation procedure for detected replication failures. A replication failure was previously undetected for 8 days — daily monitoring was clearly insufficient or not being performed. (3) No alert threshold defined — monitoring means someone must check, not that alerts are generated automatically.

7. Regulatory Compliance

NexaBank is regulated by the FFIEC and must comply with the FFIEC BCP Booklet requirements including annual DR testing, documented recovery capabilities, and board-level reporting on BCM programme health.

8. Policy Review

This policy must be reviewed annually. Last reviewed: October 2022. Next review: October 2023.

AUDIT NOTE — DELIBERATE GAP

OVERDUE: This policy review is overdue. A FFIEC-regulated institution with an overdue DR policy review and a replication failure incident in the past 12 months presents a significant regulatory and audit risk.