Document Control

Document Owner: Sarah Chen, Chief Information Security Officer
Classification: ⚠ **CONFIDENTIAL — Restricted Distribution**
Version: 2.1 **Date:** 15 July 2026
Status: Approved **Review Cycle:** Quarterly
Distribution: Executive Team, IT Operations, Business Continuity Steering Committee

Approval Signatures

Role	Name	Signature	Date
CISO	Sarah Chen	*S. Chen*	12 Jul 2026
CIO	Marcus Reed	*M. Reed*	13 Jul 2026
CEO	David Park	*D. Park*	14 Jul 2026
Head of IT Ops	Priya Nair	*P. Nair*	11 Jul 2026

1 Version History

Version	Date	Description	Author	Approved
2.1	15 Jul 2026	Updated RTO values for Core Banking System; added new DR site location in Phoenix, AZ	S. Chen	D. Park
2.0	03 Mar 2026	Full revision post-annual audit; restructured recovery tiers; added cloud failover procedures	S. Chen	D. Park
1.3	14 Nov 2025	Added third-party vendor recovery contacts; updated network topology appendix	M. Torres	S. Chen
1.2	08 Aug 2025	Incorporated lessons learned from July tabletop exercise; revised communication tree	S. Chen	M. Reed
1.1	22 May 2025	Minor corrections to server inventory and RPO targets	M. Torres	S. Chen
1.0	10 Jan 2025	Initial release of the Disaster Recovery Plan	S. Chen	M. Reed

2 Introduction

2.1 Purpose and Scope

This Disaster Recovery Plan (DRP) establishes the procedures, roles, and technical requirements for recovering critical IT systems and infrastructure operated by Nexa Financial Services. The plan covers the primary data centre located in Chicago, IL, and the secondary disaster recovery site in Phoenix, AZ.

The DRP applies to all production systems supporting the following business functions:

- Core banking and transaction processing
- Customer-facing digital platforms (web and mobile)
- Internal corporate systems (email, ERP, HRIS)
- Data warehousing and business intelligence
- Payment gateway and settlement services

Plan Activation Criteria

This plan is activated when the Chief Information Security Officer (CISO), in consultation with the Crisis Management Team, declares a disaster event. A disaster is defined as any unplanned event that results in the loss of critical IT services for more than **4 hours** or poses an imminent risk of extended service disruption.

2.2 Definitions

RTO	**Recovery Time Objective** — the maximum acceptable duration of service interruption before recovery must be complete.
RPO	**Recovery Point Objective** — the maximum acceptable age of data that can be lost, measured from the point of failure.
BCP	Business Continuity Plan.
DR Site	The secondary facility in Phoenix, AZ, designated for disaster recovery operations.
MAAO	Maximum Allowable Acceptable Outage — the absolute ceiling on downtime beyond which the organisation faces existential harm.

3 Recovery Objectives

3.1 Recovery Time and Point Objectives

The following table defines the recovery objectives for each tier of service. Systems are classified into three tiers based on business impact analysis (BIA) conducted in January 2026.

System Tier	RTO	RPO	MAAO	Critical Systems
Tier 1 — Mission Critical	⩽ 1 hr	⩽ 5 min	2 hrs	Core Banking, Payment Gateway, Customer Auth
Tier 2 — Business Critical	⩽ 4 hrs	⩽ 1 hr	8 hrs	Digital Banking Platform, CRM, Data Warehouse
Tier 3 — Operational Support	⩽ 24 hrs	⩽ 24 hrs	48 hrs	Internal Wiki, Training Systems, Dev Environments

3.2 Tier 1 — Detailed Recovery Targets

System	RTO	RPO	DR Strategy	Priority
Core Banking (NexaCore)	45 min	0 min	Hot standby — synchronous replication	1
Payment Gateway (PayFlow)	1 hr	5 min	Warm standby — async replication, 5-min sync	2
Customer Identity & Auth (ApexID)	30 min	0 min	Active-active across both sites	1
Settlement Engine	1 hr	5 min	Warm standby — async replication	3
Transaction Ledger (LedgerDB)	40 min	0 min	Hot standby — synchronous replication	1

4 Recovery Team Structure

4.1 Incident Response Team

Role	Name	Contact	Deputy
Crisis Manager	Sarah Chen, CISO	+1-312-555-0101	Marcus Reed
IT Recovery Lead	Priya Nair, Head of IT Ops	+1-312-555-0102	Tomás Reyes
Network Lead	James Okonkwo, Sr. Network Eng.	+1-312-555-0103	Lena Bergström
Database Lead	Dr. Arjun Mehta, Principal DBA	+1-312-555-0104	Yuki Tanaka
Application Lead	Olivia Fischer, VP Engineering	+1-312-555-0105	Raj Patel
Security Lead	Kevin Park, Head of InfoSec	+1-312-555-0106	Amara Osei
Communications Lead	Natalia Gomez, VP Corp Comms	+1-312-555-0107	—

4.2 Escalation Procedure

1. **Incident detected** — Any team member or monitoring system identifies a potential disaster event.
2. **Initial assessment** — IT Recovery Lead assesses scope and impact within **15 minutes**.
3. **Crisis Manager notification** — If incident meets activation criteria, CISO is notified immediately.
4. **Plan activation** — CISO declares a disaster and activates this DRP.
5. **Team assembly** — All recovery team members report to the designated war room (physical: Chicago HQ, Conference Room B; virtual: secured bridge line).
6. **Status updates** — Communications Lead issues updates every **2 hours** to stakeholders.

> **Critical: War Room Access**
>
> In the event the Chicago HQ is inaccessible, the secondary war room is located at **Nexa DR Facility, 7400 E Tierra Buena Lane, Phoenix, AZ 85260**. Virtual war room bridge: +**1-312-555-0200**, Participant Code: **482937**#.

5 Recovery Procedures

5.1 Phase 1: Declaration and Mobilisation (0–30 minutes)

Step	Action	Responsible
1.1	Confirm disaster event via monitoring dashboards and on-call engineer verification.	IT Recovery Lead
1.2	Notify Crisis Manager with initial impact assessment.	IT Recovery Lead
1.3	Crisis Manager convenes the Crisis Management Team within 15 minutes.	Crisis Manager
1.4	Declare disaster and activate this DRP. Log activation time in incident management system (NimbusIMS).	Crisis Manager
1.5	Send initial stakeholder notification via all communication channels.	Communications Lead

5.2 Phase 2: Infrastructure Failover (30 minutes–2 hours)

Step	Action	Responsible
2.1	Initiate DNS failover to DR site — update A records for `*.nexafinancial.com` to Phoenix IP range. TTL: 60 seconds.	Network Lead
2.2	Promote DR database replicas to primary. Verify data consistency against last sync timestamp.	Database Lead
2.3	Activate DR application servers and validate health checks across all Tier 1 services.	Application Lead
2.4	Re-establish VPN tunnels and configure firewall rules at DR site.	Network Lead
2.5	Run integration smoke tests on Core Banking and Payment Gateway endpoints.	Application Lead
2.6	Confirm external connectivity — validate that partner banks (Synapse Trust, Meridian Holdings) can reach DR endpoints.	Network Lead

5.3 Phase 3: Service Restoration and Validation (2–4 hours)

Step	Action	Responsible
3.1	Restore Tier 2 systems (Digital Banking Platform, CRM, Data Warehouse).	Application Lead
3.2	Execute end-to-end transaction test: deposit, transfer, withdrawal via PayFlow.	QA Lead
3.3	Validate customer authentication flows through ApexID.	Security Lead
3.4	Reconcile transaction ledger: compare Chicago ledger snapshot with Phoenix replica. Maximum acceptable discrepancy: **0 transactions**.	Database Lead
3.5	Enable customer-facing services and monitor error rates for **30 minutes** before declaring stable.	Application Lead
3.6	Issue status update to all stakeholders confirming service restoration status.	Communications Lead

5.4 Phase 4: Stabilisation and Return to Normal Operations

Return to Primary Site

Once the primary Chicago data centre is fully restored and validated, a controlled failback is executed during a pre-scheduled maintenance window. The failback procedure mirrors the failover steps in reverse order, with an additional **2-hour** data synchronisation window between site deactivation at Phoenix and activation at Chicago.

6 Communication Plan

6.1 Stakeholder Notification Matrix

Stakeholder Group	Initial	Ongoing	Channel
Executive Leadership	⩽ 15 min	Every 2 hrs	Secure SMS + Conference Call
Board of Directors	⩽ 30 min	Every 4 hrs	Email (encrypted) + Call
All Employees	⩽ 1 hr	Every 4 hrs	Internal Portal + Email
Customers	⩽ 2 hrs	Every 6 hrs	Status Page + Email + App Push
Regulators (OCC, CFPB)	⩽ 1 hr	As required	Formal filing + Designated Liaison
Partner Banks	⩽ 30 min	Every 2 hrs	Direct call to relationship manager
Media & Public	⩽ 3 hrs	As required	Press release + Social Media

6.2 Communication Templates

Initial Stakeholder Notification (Template)

Subject: **URGENT — Nexa Financial Services Service Disruption**

Body: Nexa Financial Services is currently experiencing a service disruption affecting [*list affected systems*]. Our Disaster Recovery Plan has been activated at [TIME] on [DATE]. The recovery team is working to restore services within the defined recovery time objectives. The next update will be provided by [TIME]. For urgent matters, please contact [CONTACT NAME] at [PHONE].

Sender: Natalia Gomez, VP Corporate Communications

7 Testing and Maintenance

7.1 Annual Testing Schedule

Test Type	Frequency	Next Date	Scope
Tabletop Exercise	Quarterly	15 Oct 2026	All recovery team members — scenario-based walkthrough
Tier 1 Failover Drill	Semi-Annual	01 Sep 2026	Full Core Banking and Payment Gateway failover
Tier 2 Recovery Test	Semi-Annual	15 Sep 2026	Digital Banking Platform and CRM restoration
Full-Scale Simulation	Annual	15 Mar 2027	All-hands exercise covering all three tiers
Third-Party Integration Test	Annual	01 Apr 2027	Connectivity testing with Synapse Trust and Meridian Holdings

7.2 Plan Maintenance

This document is reviewed and updated:

- **Quarterly** — by the Disaster Recovery Coordinator
- **After every test** — incorporating lessons learned and identified gaps
- **After any significant infrastructure change** — including new system deployments, architecture changes, or vendor transitions
- **After any actual disaster event** — capturing post-incident review findings

Document Control

This document is maintained in Nexa Financial Services' controlled document repository.

All printed copies are uncontrolled and valid only on the date of printing.

Refer to NimbusDocs (Ref: DRP-NEXA-2026-001) for the current approved version.

— End of Disaster Recovery Plan —