TECHNOLOGY RECOVERY RUN BOOK

Core Connectivity & Critical Systems Recovery Playbook for Credit Unions

[Credit Union Name]

Document Owner: _____ Last Updated: _____

Review this run book after every test and whenever the environment changes.

Purpose & How to Use This Run Book

This run book is your step-by-step checklist for recovering the credit union's technology environment when your primary equipment or facility is unavailable. It assumes recovery laptops are being shipped to you with a factory setup - meaning every laptop arrives clean, with no credit union configuration on it. Your job is to get from “out of the box” to “servicing members” as quickly as possible.

The priority order is intentional: core connectivity comes first. Everything else builds from there.

Priority 1: Restore secure connectivity to the core. Priority 2: Bring up the critical ancillary applications that keep the credit union running. In a crisis, work the phases in order and don't skip validation steps.

How to use it:

- Before a disaster: Fill in every blank field, contact, credential location, and application detail. A run book with blanks is a run book that fails at 2 a.m.
- During a disaster: Pull it out, start at Phase 1, and check boxes as you go. Assign a scribe to log times in Appendix C.
- After every test or environment change: Update it. Run books are living documents and should be updated far more often than your BCP.

Phase Overview - Quick Reference

Phase	Objective	Primary Owner	Target Time
1. Activate & Notify	Declare the event; get laptops shipping and MSP/core provider engaged	IT Lead / Mgmt	Hour 0–1
2. Virtual Servers	MSP verifies/restores the virtual server environment (runs in parallel)	MSP	Hours 0–24
3. Laptop Setup	Base configuration of recovery laptops	IT Lead	On arrival
4. Core Connectivity	PRIORITY ONE — secure connection to the core restored and validated	IT Lead + Core Provider	ASAP after step 3
5. Ancillary Apps	Critical non-core applications restored in priority order	IT Lead + App Owners	After step 4
6. Validate & Resume	End-to-end testing; resume member operations	All	Before opening

Key Contacts - Keep This Current

Who	Name / Company	Phone	Email / Portal	Account / Reference #
Recovery Services (Alert/Declare line)				
MSP — primary contact				
MSP — after-hours/emergency				
Core Provider — support line				
Core Provider — account rep				
Internet / Circuit Provider				
Internal: IT Lead				
Internal: Executive / Decision Maker				
Cyber Insurance / IR (if cyber event)				

Phase 1: Activate & Notify (Hour 0–1)

Goal: Declare the event, get equipment moving, and get every partner working in parallel.

Done	Step	Details / Notes (fill in yours)
☐	Assess the situation - what is down? (Facility, power, internet, hardware, cyber event)	If cyber: engage IR/insurance FIRST — steps may differ
☐	Declare with your recovery services provider - request recovery laptops (and any other assets needed)	Alert/Declare #: _____ Expected delivery: 24–48 hrs
☐	Confirm shipping address for equipment delivery	Primary: _____ Alternate: _____
☐	Notify MSP - open an emergency ticket; request virtual server status check (Phase 2)	Ticket #: _____
☐	Notify core provider - alert them a disaster has been declared and new host names will be registered	Case #: _____
☐	Assign roles: IT lead, MSP liaison, scribe/time-logger, communications lead	
☐	Notify staff via emergency notification system; identify critical staff reporting to recovery site	
☐	Pull the credentials/password vault access needed for recovery	Location of vault / break-glass credentials: _____

Phase 2: Virtual Server Environment (MSP - Runs in Parallel)

Goal: Confirm the virtual servers that host your infrastructure (domain services, file services, applications) are intact or restored. This work belongs primarily to your MSP and should run in parallel with Phases 3-4; don't wait for laptops to arrive to start it.

Done	Step	Details / Notes (fill in yours)
☐	MSP confirms status of the virtual host environment and each critical VM	Hypervisor/platform: _____
☐	If VMs are impacted: MSP initiates restore from backup or failover to replica site	Backup/replication solution: _____ RPO: _____
☐	Verify Active Directory / domain services are online	
☐	Verify DNS and DHCP services	
☐	Verify file server(s) and shared drives	
☐	Verify any application servers hosting ancillary apps (see Phase 5 list)	
☐	MSP confirms firewall/VPN appliance is available (or virtual/replacement stood up) — required for Phase 4	This is the gateway to the core — flag as critical
☐	MSP provides confirmation in writing: which servers are up, which are pending, and ETA	

Fill in ahead of time - Critical Virtual Servers:

VM / Server Name	Role (AD, file, app, etc.)	Where It Lives	Restore Method	Verified By

Phase 3: Recovery Laptop Setup

Goal: Take each laptop from factory-fresh to “ready to connect.” Repeat this checklist for every laptop; start with the one or two machines your most critical function needs — one working laptop that can service members beats ten half-configured ones.

Done	Step	Details / Notes (fill in yours)
☐	Unbox and inventory laptops; record serial numbers (Appendix B)	Qty expected: _____
☐	Complete software out-of-box setup using local admin account (skip/defer account sign-in per your standard)	Local admin naming standard: _____
☐	Connect to recovery internet (recovery-provided wireless unit, hotspot, or site connection)	SSID / connection details: _____
☐	Run software updates (critical/security at minimum — defer feature updates to save time)	
☐	Set the host name per your naming convention and record it (Appendix B)	Core provider will need these names in Phase 4
☐	Install MSP remote management/endpoint agent so MSP can support the machine remotely	Agent + install source: _____
☐	Install endpoint security / antivirus required by policy and core provider	Product: _____
☐	Install VPN client software	Client + version: _____ Config file location: _____
☐	Join domain / Azure AD (if required for core or app access)	Or document workgroup exception: _____
☐	Install browser(s) and set any required security settings	
☐	Create user profile(s) for the staff member assigned to this laptop	

Time saver to work toward: a stored image or documented “gold build” (agents, VPN client, security tools, core prerequisites) cuts this phase dramatically. Note your image location and restore steps here: _____

Phase 4: Core Connectivity - PRIORITY ONE

Goal: Re-establish the secure connection to the core and validate that transactions can be processed. Nothing in Phase 5 starts until at least one laptop is confirmed working on the core.

Done	Step	Details / Notes (fill in yours)
☐	Recreate/verify the VPN tunnel to the core (site-to-site via MSP firewall, or client VPN per your architecture)	Architecture: _____ Who builds it: _____
☐	Contact core provider: register the new laptop host names (from Appendix B) and confirm they are authorized	Provider requires: _____
☐	Confirm with core provider any IP address changes at the recovery site are whitelisted on their side	Our recovery public IP: _____
☐	Install core application software / thin client on the first laptop	Install source & steps: _____
☐	Apply required core configuration (terminal IDs, branch settings, printer mappings)	Config notes: _____
☐	Test sign-on to the core with a production user account	
☐	Validate a core function end-to-end (e.g., account inquiry, then a monitored test transaction)	Test script: _____
☐	Confirm receipt/validation printing or documented workaround	Critical printer / encoder details: _____
☐	Repeat core install/config for remaining laptops in priority order	
☐	Log completion time in Appendix C — this is your headline recovery metric	

Core connection details - fill in ahead of time:

Item	Detail
Core provider & platform	
Connection type (VPN/MPLS/etc.) and endpoints	
Who owns the firewall/VPN config (MSP or internal)	
Host name registration process & typical turnaround	
Core software install source & prerequisites	
Escalation path if sign-on fails	

Phase 5: Critical Ancillary Applications

Goal: Restore the applications outside the core that the credit union cannot operate without. Many of these are secured by IP whitelisting or device trust — which means they will not "just work" from new laptops or a new location. Work the list in priority order, and capture the access requirements for each one now, not during the event.

Done	Step	Details / Notes (fill in yours)
☐	Pull up the Critical Applications inventory (below) and confirm priority order with leadership	
☐	For each app: confirm whether the recovery site IP / new devices need to be whitelisted, and submit requests to each vendor	Vendor security contacts in table below
☐	Restore access to email and internal communications	Platform: _____
☐	Restore access to online/mobile credit unioning admin console	
☐	Restore access to wire transfer / payments systems	Extra auth requirements (tokens, callbacks): _____
☐	Restore access to ACH origination / federal payment services	
☐	Restore access to item processing / check imaging	
☐	Restore access to document imaging / signature cards	
☐	Verify each app with the business owner who uses it daily — not just an IT login test	

Critical Applications Inventory — fill in ahead of time and keep current:

Priority	Application	Vendor / URL	IP Whitelist or Device Trust? (Y/N + process)	Install or Web?	Owner	Last Tested

Phase 6: Validate & Resume Operations

Done	Step	Details / Notes (fill in yours)
☐	Run end-to-end validation: sign on, process a monitored transaction, verify it posts correctly	
☐	Confirm every critical application from Phase 5 is verified by its business owner	
☐	Confirm printing, scanning, and any critical peripherals	
☐	Brief staff: what's working, what's on workaround, who to call with issues	
☐	Notify leadership that systems are ready; make the go/no-go call to resume member operations	
☐	Send member communication if applicable	
☐	Keep the scribe logging: issues found, times, and workarounds — this becomes your after-action report	

After the Event (or Test)

- Hold a debrief within one week: What slowed us down, what was missing from this run book?
- Update every section that didn't match reality - especially whitelists, host name steps, and vendor turnaround times.
- Log the update in Appendix D and redistribute the current version.

Appendix A: IP Whitelists & Secured Websites Tracker

Every site or service locked down by IP or device - the things that break silently when you move locations.

Site / Service	URL	Restriction Type (IP / device / cert)	How to Request Access	Vendor Contact	Verified

Appendix B: Recovery Laptop & Host Name Tracker

#	Serial Number	Host Name	Assigned To / Function	Core Registered? (date)	Apps Installed

Appendix C: Recovery Time Log

Date / Time	Milestone or Issue	Owner	Resolution / Notes
	Event declared		
	Laptops received on site		
	Virtual servers confirmed/restored		
	First laptop configured		
	CORE CONNECTIVITY RESTORED		
	All critical apps verified		
	Member operations resumed		

Appendix D: Run Book Maintenance Log

Update this run book after every test, environment change, vendor change, or application change.

Date	Updated By	What Changed	Next Review Due