White
Rose

GUIDE

Business Continuity & Incident Response Guide

Document control
This document is uncontrolled when printed or downloaded and should be discarded after use. Always source the most recent version from the White Rose *Governance Fundamentals Library* and share only the document link.

Document title	**Quick Investigation**	Verbatim of above
Identification	**FORM005**	A unique identification number: letters followed by three digits.
Status	**Published**	The lifecycle status: draft/published.
Version	**1**	Major number only (0=draft; 1; 2; etc)
Approval Date	**26 February 2025**	The date this version of the document was approved
Revalidation Date	**26 August 2027**	The date the document is due for review. A maximum of two years after the approval date.
Approver	**Lee Mason**	Title of the person who owns and is responsible for the document

Revision History		
Revised by	Revisions/changes/comments	Date re-published
Samantha Mason	**First drafting**	**26 February 2025**

1. Purpose

This guide sets out how White Rose Loan Processing ("WRLP") maintains continuity of operations and protects client outcomes in the event of a disruption (e.g., power outage, internet/telco failure, system outage, natural event, or staff unavailability). It defines roles, response actions, communication protocols, and recovery objectives to minimise service disruption to brokers, aggregators, and clients.

2. Scope

This policy applies to all WRLP staff/contractors, systems, and processes involved in loan processing, document management, communications, and compliance.

3. Principles

- Client and broker continuity first: Maintain processing momentum and meet critical deadlines.
- Safety & security: Protect data confidentiality, integrity, and availability at all times.
- Redundancy, not reliance: Avoid single points of failure in systems, power, and connectivity.
- Clear communication: Proactive, timely updates to affected stakeholders.
- Continuous improvement: Test, review, and refine.

4. Roles & Responsibilities

Business Owner – Oversees activation, internal/external communications, and post-incident review.

All Staff/Contractors: Follow procedures, maintain updated contact details, and report incidents promptly.

5. Business Impact & Recovery Objectives

5.1 Critical Activities

- Loan file intake, verification, and submission
- Time-sensitive lender/broker communications
- Compliance recordkeeping and document management

5.2 Recovery Objectives

- RTO (Recovery Time Objective):

- Connectivity outage (internet/telco): ≤ 1 hour via failover (mobile hotspot / secondary ISP)
- Power outage: ≤ 1 hour via battery/relocation
- Core platform outage (e.g., CRM/Doc store): ≤ 4 hours via vendor failover/alternative workflow

6. Preventative Controls & Redundancy

6.1 Infrastructure

- **Power:** UPS/battery backup for primary workstation; portable power bank for mobile devices.
- **Connectivity:** Dual connectivity (primary ISP + 4G/5G mobile hotspot).

- **Devices:** Two capable work devices (primary + backup laptop or tablet) configured for secure access.

6.2 Systems & Data

- **Cloud-first stack:** All operational data (emails, files, tasking) in secure cloud platforms with MFA and role-based access.
- **Backups:** Documents & platform data protected by vendor redundancy/version history; (noting White Rose Loan Processing does not store any external client information).
- **Security:** MFA enforced, device encryption, screen lock, least-privilege access.
- **Vendors:** Maintain up-to-date records of vendor SLAs and status pages; subscribe to incident notifications.

6.3 People & Process

- **Cross-skilling:** Key processes documented so another team member or the owner can execute.
- **Standard Operating Procedures (SOPs):** Stored in WRLP cloud storage; reviewed annually.
- **Contact Alternatives:** Multiple channels maintained (mobile, email, MS Teams/Zoom).

7. Incident Categories & Triggers

- **Category A – Minor:** Disruption ≤ 60 minutes, no deadline impact.
- **Category B – Moderate:** Disruption 1–4 hours, potential deadline impact.
- **Category C – Major:** Disruption > 4 hours or security concern, high deadline impact.

Note: Business owner may activate this policy at Category B or C, or at discretion for critical files.

8. Response Procedures (Playbooks)

8.1 Power Outage (Local)

1. **First 5–10 minutes:** Switch to battery power; keep modem/router on UPS. Save open work; confirm cloud autosave is active.
2. **If unresolved after 15 minutes:** Move to backup device if required. If power is likely extended, relocate to an alternate site with power (e.g., co-working space/external site).
3. **Communications:** For Category B/C incidents, send broker update.
4. **Recovery:** Resume normal operations; log incident.

8.2 Internet/Telco Outage

1. **Immediate failover:** Switch to mobile hotspot (4G/5G) or secondary ISP (if available).
2. **If hotspot unavailable:** Relocate to alternate site with reliable internet.
3. **Communications:** Notify brokers for Category B/C; provide ETA.
4. **Recovery:** Verify no data sync issues; resume.

8.3 Cloud Platform Outage (CRM/Docs/Email)

1. **Verify status:** Check vendor status page and subscribe to updates.
2. **Workaround:** Continue using unaffected systems; use local working folder with offline copies for documents where permissible, then sync on restore. Log critical tasks in temporary task tracker (e.g. spreadsheet in secondary platform).

3. **Escalation:** If > 60 minutes or impacts deadlines, issue broker update and coordinate alternate submission pathways if available.
4. **Recovery:** Reconcile offline and online records; confirm version integrity.

8.4 Staff Unavailability (Short-Term)

1. **Activation:** Onboard interim resources (contractor).
2. **Handovers:** Use SOPs and daily tasks for continuity.
3. **Communications:** Update impacted brokers on assigned contact and timeframes.

8.5 Information Security Considerations

- WRLP will never move client data to personal or unapproved systems.
- WRLP will Use VPN where configured; maintain MFA at all times.
- WRLP will report any suspected data exposure immediately to Business Owner and follow data breach procedure.

9. Communication Protocols

- **Audience:** Brokers, aggregator, key third parties (as needed).
- **Channels:** Email + mobile; if email impacted, use mobile SMS/voice and Teams/Zoom.
- **Cadence:** Initial notice within 30 minutes for Category B/C; updates every 3 hours or on material change.
- **Tone:** Clear, calm, and solution-focused; include ETA and workaround.

10. Testing & Review

- **Tabletop test:** Twice per year (simulate power and telco outages).
- **Live failover check:** Quarterly test of mobile hotspot and alternate location login.
- **Data restore check:** Semi-annual verification of version history/restore capability.
- **Post-incident review:** For any Category B/C event, document cause, actions, timeline, outcomes, and improvements within 5 business days.

11. Documentation & Records

WRLP will maintain incident logs, test records, vendor SLAs/status links, and SOPs.

12. Compliance & Privacy

WRLP adheres to applicable privacy and data protection obligations. BCP actions must comply with client confidentiality, secure handling of sensitive information, and contractual requirements with brokers, aggregators, and lenders.