



॥ धर्मेण न्यायः स्थाप्यते ॥
PDR COURT

PDR ORGANIZATION PRIVATE LIMITED
BUSINESS CONTINUITY POLICY

Document Control

Field	Details
Company	PDR Organization Private Limited
Document	BCP / DRP / Cyber Incident Response / ODR Continuity
Version	1.0
Policy Owner	Business Continuity Officer / Management
Approval Authority	Board of Directors / Authorized Management
Review Frequency	At least annually and after material incidents or major changes
Classification	Internal / Confidential

Document Index

No.	Document	Status
1	Business Continuity Management Policy	Master Policy
2	Business Impact Assessment (BIA) Framework	Operational Register
3	Risk Assessment & Risk Register	Operational Register
4	IT Disaster Recovery Plan	Technical Recovery Plan
5	Cyber Incident Response Plan	Security Response Plan
6	ODR Operational Continuity SOP	Critical Operations SOP
7	Legal Proceedings Continuity Protocol	Arbitration/Conciliation Protocol
8	Communication & Escalation Matrix	Incident Communications
9	Critical Vendor Continuity Plan	Third-Party Resilience
10	BCP Testing & Drill Procedure	Assurance
11	Post-Incident Review Template	Lessons Learned
12	Employee BCP Quick Reference	Awareness / Emergency Guide

1. Business Continuity Management Policy

PDR Organization Private Limited (“PDR” or “Company”) operates technology-enabled Online Dispute Resolution (ODR), arbitration and conciliation services. This Policy establishes the framework for maintaining critical services during disruption and restoring normal operations in a controlled manner.

1.1 Purpose

Protect clients, parties, arbitrators/conciliators, employees and critical records; minimise service interruption; preserve confidentiality and integrity; and provide a structured recovery framework.

1.2 Scope

Applies to all employees, critical departments, ODR applications, databases, cloud infrastructure, document storage, communications, online hearings, client operations, postal operations and critical third parties.

1.3 Governance

Management approves the framework. The Business Continuity Officer (BCO) coordinates it. Department Heads own continuity procedures for their functions. Technology owns technical recovery and security response.

1.4 Principles

Availability, integrity, confidentiality, resilience, documented alternatives, proportional response, stakeholder protection and continual improvement.

1.5 Critical Business Functions

- Arbitration and conciliation case administration
- Arbitrator/neutral nomination, acceptance and allocation
- Notices and party communications
- Online hearings and hearing coordination
- Pleadings, evidence, orders and award records
- Client case intake, processing and MIS
- Email, SMS, WhatsApp and IVR communications
- ODR platform, application, database and document storage
- Postal dispatch and tracking where applicable

1.6 Initial Recovery Objectives

Function	Target RTO	Target RPO
ODR platform	4 hours	1 hour
Case database	4 hours	1 hour
Case documents	8 hours	4 hours
Corporate email	4 hours	4 hours
SMS/WhatsApp	8 hours	4 hours
Online hearings	8 hours	N/A
Client case processing	8 hours	4 hours
Website	8 hours	24 hours
Internal HR/Admin	24 hours	24 hours

RTO = Recovery Time Objective. RPO = Recovery Point Objective. These are management targets and may be revised following the BIA, technical assessment and contractual commitments.

1.7 Continuity Activation

1. Detect and log the incident.

2. Assess severity, affected systems/functions and immediate risks.
3. Activate the relevant continuity or disaster recovery procedure.
4. Protect people, case records, credentials and evidence.
5. Notify internal stakeholders and affected external stakeholders where required.
6. Restore critical services in priority order.
7. Validate data integrity and reconcile temporary records.
8. Return to normal operations and conduct a post-incident review.

1.8 Review and Testing

The BCP shall be reviewed at least annually and after material incidents, major technology changes, significant vendor changes or relevant legal/regulatory developments. Backup restoration, cyber response, alternate hearing, remote working and communication procedures shall be tested periodically.

2. Business Impact Assessment (BIA) Framework

The BIA shall be maintained by process owners and reviewed at least annually. Each process shall be rated for operational, legal/procedural, client, financial, confidentiality and reputational impact.

Process	Criticality	Max Tolerable Disruption	Minimum Resource	Key Dependency
ODR case management	Critical	4–8 hrs	Operations + IT	Application + DB
Online hearings	Critical	8 hrs	Ops + Neutral	Video platform + internet
Notices/communications	Critical	8 hrs	Communication Team	Email/SMS/WhatsApp/IVR
Case documents	Critical	8 hrs	Ops + IT	S3/document store
Client intake/MIS	High	24 hrs	Client Ops	Database + reports
Postal dispatch	High	24–48 hrs	Postal Team	Printer/courier
HR/Admin	Medium	48 hrs	Admin/HR	HRMS/email

Each process owner shall maintain a current contact list, alternate resource, manual workaround and dependency list.

3. Risk Assessment & Risk Register

Risk scoring may use Likelihood (1–5) × Impact (1–5). Scores of 15–25 should generally be treated as high/critical and reviewed by Management.

Risk	Potential Impact	Preventive / Mitigating Controls	Owner	Priority
Cloud/service outage	Platform unavailable; hearings delayed	Backups, monitoring, recovery runbook, alternate hearing platform	Technology	High
Database corruption/loss	Case records unavailable or inaccurate	Scheduled backups, access controls, restoration tests	Technology	Critical
Ransomware/cyberattack	Operational and confidentiality impact	MFA, endpoint controls, least privilege, backups, incident response	Technology/InfoSec	Critical
Email outage	Notice/client communication delayed	Alternate approved channel, provider support, templates	Communications	High

SMS/WhatsApp/IVR outage	Party reachability reduced	Alternate channels and vendor escalation	Communications	High
Internet/power outage	Office operations/hearings interrupted	UPS, alternate connectivity, remote work	Admin/IT	Medium
Key employee unavailable	Critical activity delayed	Cross-training, documented SOPs, backups	Management	High
Vendor failure	Dependent service unavailable	SLA, escalation contacts, alternative provider assessment	Management/IT	High
Office inaccessible	Staff unable to work	Remote work and alternate location arrangements	Management	Medium
Domain/DNS failure	Website/email/API access affected	Registrar controls, documented DNS, recovery access	IT	High

The register shall be updated after material incidents and at least annually.

4. IT Disaster Recovery Plan

4.1 Recovery Priorities

- Establish incident command and preserve evidence.
- Confirm security of the recovery environment.
- Restore network/connectivity and access controls.
- Restore database services.
- Restore application/server services.
- Restore document/object storage and verify integrity.
- Restore authentication and integrations.
- Restore email and communication integrations.
- Validate case access, documents and critical workflows.
- Release systems to Operations after technical validation.

4.2 Backup Requirements

- Critical databases and case records shall be backed up on a defined schedule.
- Backups shall be access-controlled and protected from unauthorised deletion.
- Where feasible, at least one recovery copy should be logically or physically separated from the production environment.
- Restoration tests shall be documented.
- Backup failures shall generate an operational alert and be remediated.

4.3 Temporary Manual Operations

During an outage, Operations may maintain an approved temporary tracker containing only the minimum information required to continue critical work. Temporary records must be reconciled into the official system after restoration and securely disposed of when no longer required.

5. Cyber Incident Response Plan

5.1 Trigger Events

- Ransomware or malware
- Suspected unauthorised access
- Credential compromise
- Data leakage or exfiltration
- Suspicious administrative activity
- Website/application compromise
- Loss of device containing Company data
- Third-party security incident affecting PDR

5.2 Response Phases

- Identify and report immediately.
- Triage severity and affected assets.
- Contain the incident by isolating affected accounts/systems.
- Preserve logs, evidence and relevant records.
- Eradicate malicious access or software.
- Recover using clean, verified systems/backups.
- Validate security and data integrity.
- Notify management, clients or authorities where legally/contractually required.
- Conduct post-incident review.

5.3 Rules During Cyber Incidents

- Do not delete logs or evidence.
- Do not use compromised credentials.
- Do not communicate with attackers unless specifically authorised.
- Do not restore infected backups without security assessment.
- Do not conceal a suspected material incident.
- External communications must be authorised.

6. ODR Operational Continuity SOP

6.1 Platform Outage

- Operations confirm outage with Technology.
- Open an incident ticket and record start time.
- Identify affected cases/hearings.
- Technology provides estimated restoration status.
- For urgent hearings, Operations coordinates an approved alternate video platform where appropriate.
- Notify arbitrator/conciliator and affected parties where the outage materially affects the proceeding.
- Maintain a temporary hearing/case log.
- Once restored, reconcile all records and communications into the official case file.
- Close incident after Operations and Technology sign-off.

6.2 Notice/Communication Failure

If a primary communication channel fails, use an approved alternative channel consistent with the case procedure, contractual requirements and applicable law. The original communication attempt and the alternative communication shall be recorded in the case management record.

6.3 Arbitrator/Neutral Availability

If an appointed neutral becomes unavailable during a continuity event, Operations shall escalate to the authorised arbitration administration team and follow the applicable appointment/procedural rules. No employee shall independently alter an appointment or substantive procedural direction without proper authority.

7. Legal Proceedings Continuity Protocol

This Protocol applies to arbitration and conciliation matters administered by PDR where a technology, communication, premises or other disruption may affect the proceeding.

7.1 Hearings

- The disruption shall be documented.
- The arbitrator/neutral shall determine appropriate procedural directions concerning adjournment, continuation or alternative arrangements.
- PDR shall facilitate communication and technology support.
- Where an alternate platform is used, access shall be limited to authorised participants.
- Hearing records and documents shall be preserved and subsequently incorporated into the official case file.

7.2 Pleadings and Evidence

- Do not discard submissions received during an outage.
- Preserve date/time and sender information where available.
- Use approved alternative channels only when necessary.
- Reconcile all submissions into the official case repository after restoration.

7.3 Notices and Service Records

- Maintain records of attempted and successful communications.
- Record channel, date/time and relevant delivery information.
- Where a procedural or legal requirement is affected by an outage, escalate to the authorised legal/administrative team and the arbitrator/neutral as appropriate.

7.4 Orders and Awards

Drafts, procedural orders and awards shall be protected as critical records. Temporary storage during an outage must use approved access-controlled locations. Final records shall be placed in the official case repository after restoration.

8. Communication & Escalation Matrix

Event	Internal Notification	External Notification	Target
Critical platform outage	BCO + IT + Operations + Management	Affected clients/parties/neutrals where material	As soon as practicable
Cyber incident	IT/InfoSec + Management + Legal/Compliance	As required by law/contract	Immediate escalation
Hearing disruption	Operations + IT	Arbitrator/parties affected	Before/at earliest

			opportunity
Communication vendor outage	Communications + IT	Affected clients/parties if material	As needed
Office inaccessible	Management + Admin/HR + IT	Clients only if service impact	Immediate
Major vendor outage	IT + Management	Affected clients if material	As needed

The live emergency contact list shall be maintained separately and must not be hard-coded into this public-facing copy. It should include names, roles, primary/secondary phone numbers and approved email addresses.

9. Critical Vendor Continuity Plan

Vendor / Service Category	Dependency	Primary Failure Action	Alternative / Escalation
Cloud infrastructure	Servers/database/storage	Open vendor incident; activate DR	Documented recovery environment / vendor escalation
Object/document storage	Case documents	Validate availability and backups	Recovery copy / support escalation
Email provider	Client/party communication	Check service status; escalate	Approved alternate communication
SMS provider	Notice/reminder delivery	Escalate provider	Alternate channel
WhatsApp Business provider/API	Party communication	Escalate provider	SMS/email/call where appropriate
IVR/telephony	Calling operations	Escalate provider	Alternate calling/SMS
Video conferencing	Online hearings	Use alternate approved platform	Second approved platform
Domain/DNS/Registrar	Website/email/API routing	Escalate registrar/DNS	Documented DNS recovery procedure

Management/IT shall maintain a live vendor register containing contract/SLA information, support contacts, escalation levels, renewal dates and criticality.

10. BCP Testing & Drill Procedure

10.1 Minimum Test Programme

Test	Suggested Frequency	Evidence
Backup restoration	Quarterly	Restore log + screenshot/report
Cyber tabletop exercise	Half-yearly	Scenario, attendees, actions
Alternate hearing platform	Quarterly	Test meeting + checklist
Remote working continuity	Half-yearly	Attendance + issue log
Critical vendor escalation	Annual	Escalation test record
Full BCP exercise	Annual	Exercise report + corrective actions

10.2 Test Report Template

Field	Entry
Date	
Scenario	
Participants	
Systems/Processes Tested	
Expected Recovery Time	
Actual Recovery Time	
Data Loss / RPO Result	
Issues Identified	
Corrective Action Owner	
Due Date	
Management Sign-off	

11. Post-Incident Review Template

Field	Details
Incident ID	
Date/Time Started	
Date/Time Resolved	
Severity	
Affected Services	
Root Cause	
Business Impact	
Client/Case Impact	
Data Impact	
Actions Taken	
What Worked	
What Failed	
Corrective Actions	
Owner & Due Date	
Management Approval	

12. Training and Awareness

PDR will ensure that awareness and training programs, in accordance with Bank's Policy for participating teams are conducted to: -

- Communicate importance of the plan.
- Creating awareness about responsibilities and safety.

13. Employee BCP Quick Reference

During any suspected major disruption:

- Protect yourself and follow emergency instructions.
- Immediately report the incident to your reporting manager / designated incident channel.
- Do not delete, alter or conceal business records.
- Do not share confidential case information through unapproved channels.

- Do not use personal storage for Company/case records unless expressly authorised as an emergency workaround.
- Do not make public statements about incidents.
- Follow instructions from the Incident Response / BCP Team.
- Record important actions, communications and times.
- After recovery, reconcile temporary records into the official system.

Emergency Information to Be Maintained Separately

- BCO contact
- Technology/InfoSec escalation
- Management escalation
- Operations escalation
- Legal/Compliance escalation
- Critical vendor contacts
- Alternate hearing platform details
- Backup/recovery administrator contacts
- Office/emergency services information

,