Disaster Recovery Plan

Pronounced80 Solutions Limited

Freeing business from the tyranny of legacy software

Version 1.0 | Effective: May 2026 | Review: Annual

1. Purpose

To recover IT systems and data following a disruptive event.

2. Scope

Devices, identity, email, source control, cloud platforms and the data required to deliver services.

3. Approach

We operate a remote-first, cloud-first model. Critical systems are SaaS / PaaS backed by provider-native resilience and backups, minimising on-premise recovery scope.

4. Systems and Recovery Approach

System	Recovery approach
Microsoft 365 (email, files)	Provider-native resilience; restore via M365 retention/recycle bin and version history.
Microsoft Entra ID	Provider-native; account recovery via documented break-glass procedure.
GitHub / Azure DevOps	Distributed Git copies; provider-native resilience; periodic export of critical repos where required.
Azure / AWS workloads (when delivering for clients)	Designed per client architecture; backups, snapshots and IaC enabling rebuild.
Endpoint device	Reimage/replace; data restored from cloud-synced storage.

5. Recovery Objectives (indicative)

- Email and identity: within 1 business day.
- Source control and tooling: within 1 business day.
- Endpoint replacement: within 2 business days.
- Client environments: per client-agreed RTO/RPO.

6. Backups

- Cloud-native backup, versioning and recycle bin used for productivity data.
- Client environments use provider-native backup/snapshot features per design.

7. Network Failures

- Primary internet via fixed broadband; failover via mobile tethering (4G/5G).
- Client VPN access tested when first established and on material change.

8. Testing

- Periodic restore test for selected files/repos at least annually.
- Account recovery procedure verified at least annually.
- Findings logged and acted upon.

9. Communication

Clients are notified promptly where DR invocation may affect their services.