Disaster Recovery Plan – Legacy & Legacy Portal

Document Owner: Chief Technology Officer, CTT Group
Version: 1.0 Draft
Date: 8 June 2025

---

1. Purpose of This Document

This Disaster Recovery Plan (DRP) sets out how *Legacy* and *Legacy Portal* services will be restored in the event of a failure, outage, or disaster.
Our aim is simple: **to get you working again as quickly as possible, with minimal disruption, while protecting all client data.**

---

2. Systems Covered

1. **Legacy**
   - A Windows-based application installed on our clients' PCs.
   - Used by will-writing professionals and estate planners to create legal documents and manage client cases.
   - Connects securely to our servers in UK-based secure data centres.
2. **Legacy Portal**
   - Accessible via web browser or mobile app (Android/iOS).
   - Used by your clients to view documents, share information, and communicate with you.
   - Hosted on the *Alpha Cloud* in AWS's UK London region.

---

3. How the Systems Work (in simple terms)

Legacy

- The software you run on your PC talks securely to our server in a UK secure data centre.
- That server's contents are **continuously copied** to another UK data centre.
- Nightly backups are taken of both the application server and its database.

- The database is stored in SQL Server, on a separate dedicated database server, which is also backed up nightly to the secondary data centre.

Legacy Portal

- When you or your clients use the Portal (web or app), the request goes to our *Alpha Cloud* servers hosted by AWS in London.
- The application connects to a secure SQL Server database hosted in AWS RDS (also in the UK).
- The database is backed up every night using AWS “snapshots”.
- If the *Alpha Cloud* fails, we can re-create and re-host the application on a new AWS server within **2 hours**.

4. Types of Disruptions We Plan For

We plan for:

1. **Server failure** – hardware or software issues stopping a server from working.
2. **Network outage** – internet or data centre connectivity problems.
3. **Data corruption or accidental deletion** – human error, system bug, or cyber incident.
4. **Cloud service failure** – AWS or Alpha Cloud unavailability.
5. **Complete site failure** – disaster affecting a whole data centre (fire, flood, power loss, etc.).

5. Recovery Strategy

5.1 Legacy

Failure Type	Recovery Steps	Estimated Recovery Time
Primary server failure	Switch to continuously replicated secondary server in another UK data centre	**< 1 hour**
SQL Server failure	Use secondary SQL Server in backup data centre	**< 1 hour**

Failure Type	Recovery Steps	Estimated Recovery Time
Data corruption	Restore from previous night's backup	**< 4 hours**
Complete data centre outage	Switch all services to secondary UK data centre	**< 2 hours**

Key Points:

- Because the data is always copied in real time to another site, most failures can be recovered very quickly.
- Backups are stored securely off-site to guard against corruption or ransomware.

5.2 Legacy Portal

Failure Type	Recovery Steps	Estimated Recovery Time
Alpha Cloud application failure	Deploy backup version of the application to a new AWS IIS server	**< 2 hours**
AWS RDS database issue	Restore from latest snapshot backup	**< 4 hours**
AWS London region outage	Deploy application and database to alternative AWS UK region	**4–8 hours**

Key Points:

- AWS hosting gives us resilience but we also plan for rare full-region outages.
- Mobile apps will automatically connect to the restored system when it is back online.

---

6. Communication During an Incident

In the event of a disruption:

1. We will **email all affected clients** within 30 minutes of confirming the issue.
2. We will post regular updates on our **status page** (URL provided to clients in advance).

3. Once services are restored, we will send a **full incident summary** including what happened, how it was resolved, and what changes will be made to prevent recurrence.

---

7. Testing & Review

- We test our disaster recovery procedures for both *Legacy* and *Legacy Portal* **twice a year**.
- After every test or real incident, we review and update this plan.
- Any changes to our infrastructure that affect recovery are incorporated immediately.

---

8. Responsibilities

- **CTO** – Overall responsibility for disaster recovery.
- **Infrastructure Team** – Carry out recovery steps for servers, databases, and cloud environments. Currently Emerald IT
- **Support Team** – Communicate with clients and provide front-line assistance.
- **Security/Data Officer** – Ensure data integrity and compliance during recovery.

---

9. Summary

Our infrastructure has been built to **withstand most common failures** without you even noticing. In the rare case that something does go wrong, this plan ensures we can recover quickly, keep you informed, and protect your data.

Your business continuity is our priority.