Disaster Recovery Plan (DRP)

Digitech Branding (Dynasend Platform)

---

1. Purpose and Scope

This Disaster Recovery Plan (DRP) establishes the technical processes used by Digitech Branding ("the Company") to recover systems and data in the event of a disaster affecting the Dynasend platform.

The scope includes:

- The **Dynasend web application** (manage.dynasend.net) hosted in AWS
- The **Office 365 Outlook add-in**
- Supporting company services hosted in **AWS** and **Microsoft 365**
- Customer "business card" data processed by the platform

---

2. Objectives

- Restore Dynasend services within defined timelines after a disaster
- Minimize downtime and data loss through AWS resilience features
- Ensure recovery of data from encrypted backups
- Provide transparent communication to customers

Recovery Point Objective (RPO): ≤ 24 hours
Recovery Time Objective (RTO): ≤ 24 hours

---

3. Roles and Responsibilities

- **CEO/CSO (US Citizen)**
    - Activates the DRP in the event of a disaster
    - Notifies customers of service disruption and recovery status
    - Authorizes restoration actions
- **Developer / Technical Lead**

- Executes AWS recovery steps (infrastructure redeployment, data restoration)
- Validates system integrity after recovery
- Documents technical lessons learned

---

4. Disaster Scenarios

The following scenarios are considered within scope:

1. **AWS service outage** in a region or availability zone
2. **Application failure** due to deployment error or cyber incident
3. **Database/data corruption** requiring restoration from backup
4. **Loss of company devices** affecting access to AWS environment

---

5. AWS Disaster Recovery Procedures

5.1 Application Infrastructure (EC2 / Containers / Serverless)

1. Assess whether AWS reports an outage affecting the production region.
2. If outage is AZ-specific, redeploy services in a different availability zone.
3. If region-wide, redeploy application stack into the designated secondary US AWS region.
4. Update DNS (Route 53) records to point to restored services.
5. Validate service availability.

5.2 Database / Data Layer

1. Identify time of failure.
2. Retrieve latest encrypted snapshot from AWS backup storage (minimum daily).
3. Restore database instance in secondary availability zone or region.
4. Apply transaction logs if available to minimize data loss.
5. Validate data integrity and reconcile with monitoring logs.

5.3 Backups

- Backups are encrypted (AES-256) and stored in a geographically separate US AWS region.
- Retention: 30 days.
- Backup restoration tests occur semi-annually.

5.4 Identity and Access Management (IAM)

- Recreate IAM roles and policies in new region if failover required.
- Enforce MFA for AWS root and IAM user accounts.

5.5 End-User Devices

- If a device used to access AWS is lost/stolen:
    - Revoke device session and credentials from AWS IAM.
    - Provision access from alternate device.

---

6. Disaster Recovery Testing

- Restoration from AWS snapshots is tested semi-annually.
- Failover simulation (switch to backup environment) is tested at least once every 24 months.
- Any issues discovered during tests are documented and resolved.

---

7. Communication Plan

- Customers notified of disaster events within **24 hours**.
- If customer data is impacted, notification occurs within **48 hours** (per IT Security Policy).
- Recovery status updates provided daily until resolution.

---

8. Plan Review and Maintenance

- The DRP is reviewed annually and updated as needed.

- Any real disaster or recovery event will trigger a post-incident review and DRP update.

Conclusion

This Disaster Recovery Plan ensures that Digitech Branding can restore the Dynasend platform within defined recovery objectives, leveraging AWS redundancy and encrypted backups to minimize disruption to customers.