**Business Continuity Plan (BCP)**

**Digitech Branding (Dynasend Platform)**

---

## 1. Purpose and Scope

This Business Continuity Plan (BCP) describes the measures Digitech Branding ("the Company") uses to maintain essential business operations during a disruption.

The scope includes:

- The Dynasend web application (manage.dynasend.net)
- The Outlook add-in for Microsoft 365
- Company systems, accounts, and data hosted in AWS and Microsoft 365
- All customer "business card" data processed by the platform

---

## 2. Objectives

- Maintain availability of customer-facing services
- Recover customer data and operations within defined timelines
- Protect the confidentiality, integrity, and availability of information assets
- Meet contractual obligations, including GDMS requirements

---

## 3. Roles and Responsibilities

- **Chief Executive Officer (CEO) / Chief Security Officer (CSO)**
  - Owns and activates the BCP
  - Leads customer and vendor communications
  - Approves recovery and failover actions
- **Developer / Technical Lead**
  - Executes technical recovery tasks
  - Maintains system recovery documentation

    - Provides updates on restoration progress

---

**4. Risk Scenarios**

The Company has identified these risk categories:

1. **Application outage** (e.g., AWS region failure, service interruption)
2. **Data loss/corruption** (e.g., software error, misconfiguration, cyber incident)
3. **Loss of company devices or facilities** (e.g., theft, fire, natural disaster)
4. **Loss of personnel availability** (illness, accident, travel interruption)

---

**5. Recovery Strategies**

**5.1 Application and Infrastructure (AWS)**

- The Dynasend platform is hosted on **Amazon Web Services (AWS)**.
- Services are deployed with **multi-AZ redundancy** for high availability.
- In the event of a failure in one AWS availability zone, services can be restarted in another.
- Recovery Time Objective (RTO): ≤ 24 hours.

**5.2 Data Backup and Recovery**

- Daily backups of customer and application data are taken automatically.
- Backups are **encrypted (AES-256)** and stored in geographically separate AWS regions within the United States.
- Backup retention: 30 days.
- Backup restoration is tested at least **twice per year**.
- Recovery Point Objective (RPO): ≤ 24 hours.

**5.3 End-User Devices**

- Company laptops are encrypted and secured with MFA-protected cloud accounts.
- If a device is lost or stolen, access to customer systems can be restored from a replacement device.

### 5.4 Personnel Availability

- In the absence of one staff member, the other assumes critical responsibilities.
- Key recovery and operational tasks are documented to support cross-coverage.
- If both staff are unavailable, AWS automation and resilience measures will continue protecting customer data until one staff member resumes operations.

---

## 6. Communication Plan

- Major service disruptions will be communicated to affected customers within **24 hours**.
- If customer data is impacted, notification will occur within **48 hours**, consistent with the IT Security Policy.
- Customers will be updated periodically until resolution.
- Communication will occur via email to the customer's designated point of contact.

---

## 7. Plan Testing and Maintenance

- The BCP is reviewed annually by the CEO/CSO.
- AWS backup restoration tests are conducted semi-annually.
- Lessons learned from incidents or tests are incorporated into future revisions.

---

## 8. Plan Activation

The CEO/CSO may activate this plan if a disruption significantly impacts Company operations or customer services.

---

## Conclusion

This Business Continuity Plan demonstrates Digitech Branding's ability to leverage AWS infrastructure, automated redundancy, and documented recovery procedures to maintain service availability and recover operations in the event of a disruption.