# Dataco Global Business Continuity and Disaster Recovery Policy

**Purpose**
This policy establishes procedures, responsibilities, and standards to ensure Dataco Global can withstand and recover from significant business disruptions, disasters, or security incidents. The objective is to maintain essential functions and minimize operational, financial, and reputational impacts.

**Scope**
This policy applies to all Dataco Global employees, contractors, and stakeholders, and covers all business units, IT systems, facilities, and third-party dependencies.

**Definitions**

- *Business Continuity (BC)*: The capability to continue essential functions during and after a disruption.
- *Disaster Recovery (DR)*: The process to restore IT systems, data, and infrastructure within defined timeframes following a disruption.

**Policy Statements**

**1. Risk Assessment and Business Impact Analysis (BIA)**

- Dataco Global will conduct a formal risk assessment and BIA annually (every 12 months) to identify critical business functions, potential threats, and quantify impacts. The risk assessment and BIA report must be completed and submitted by Q1 of each calendar year[5].
- All assets supporting mission-critical functions must be classified and documented within the risk register, updated semi-annually.

**2. Recovery Objectives**

- Recovery Time Objective (RTO): All mission-critical systems must be restored within 4 hours of a declared disaster.
- Recovery Point Objective (RPO): Data loss for mission-critical applications must not exceed 30 minutes.

**3. Data Backup and Storage**

- Full data backups of all production systems must occur daily, with incremental backups every 2 hours.
- At least one set of encrypted backup data must be stored offsite at a geographically distinct location.
- Backup restoration tests must be performed quarterly, with a pass rate of 100% for mission-critical data.

### 4. Alternate Operations Site

- A fully equipped alternate operations site must be available and operational within 6 hours of primary site failure.
- The alternate site must provide capacity for at least 80% of critical staff roles.

### 5. Communication

- All employees must have access to updated emergency contacts and communication protocols.
- Internal notification of any business disruption must occur within 30 minutes of incident discovery.

### 6. Training and Testing

- Mandatory annual BC/DR training for all employees, with 100% participation tracked and documented.
- Full-scale BC/DR plan exercises must occur at least twice per year, with incident response team participation rate at 100%.
- Any identified gaps during exercises must result in actionable remediation within 30 days.

### 7. Plan Review and Maintenance

- The Business Continuity and Disaster Recovery Plan (BCDRP) must be reviewed and updated at minimum every 12 months, or within 7 days following a significant organizational or technological change.
- All revisions to the policy must be approved by the Board of Directors.

### 8. Third-Party Dependencies

- All critical third-party vendors must provide evidence of their own BCDR capabilities and test results annually.
- Contracts with third parties must stipulate a maximum allowable downtime of 4 hours for services impacting mission-critical functions.

### 9. Regulatory and Compliance

- The BCDRP must comply with all relevant legal, regulatory, and contractual obligations, with annual compliance audits.

### Enforcement

- Non-compliance with this policy may result in disciplinary action, up to and including termination.

> **Note:** This policy has been generated specifically for a hackathon and has no relation with Syngenta or any other company.