DUNCAN YOUNG CONSULTING
leadership & communication

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

Purpose

The purpose of this policy is to establish a framework for maintaining and restoring Duncan Young Consulting's critical business operations in the event of a disruption. This includes procedures to minimize the impact of emergencies, natural disasters, cybersecurity incidents, and other unforeseen events that may interrupt services to clients or internal operations.

Scope

This policy applies to:
All Duncan Young Consulting employees, contractors, and management staff.
All company facilities, IT systems, and digital platforms used for corporate training delivery.
All business functions related to client service, training program delivery, data management, and financial operations.

Objectives

- Ensure the safety of staff and clients.
- Maintain critical business functions with minimal disruption.
- Protect company and client data.
- Recover normal operations as quickly as possible.
- Comply with legal, regulatory, and contractual obligations.

Key Roles and Responsibilities

Role	Responsibility
Directors	Approves the BCDR policy and leads crisis management decisions.
Operations Manager	Coordinates continuity planning, communication, and recovery efforts.
IT Administrator (and vendor)	Manages data backup, system restoration, and cybersecurity response.
All Employees	Follow emergency procedures and report incidents immediately.

Risk Assessment

- Duncan Young Consulting has identified the following potential risks:
- Loss of office access due to fire, flood, or power outage.
- Data loss from hardware failure, cyberattack, or accidental deletion.
- Unavailability of key staff or trainers.
- Internet or platform outages affecting online training sessions.
- A risk assessment will be conducted annually to update mitigation strategies.

Business Continuity Strategy

Remote Operations

- Staff can perform all essential functions remotely using laptops and secure cloud systems.
- Communication channels: Microsoft Teams / Zoom / company email.
- All employees must have remote access credentials and training.

Alternate Work Locations

- In case of office inaccessibility, work will continue from home offices or coworking spaces.

Data Backup

- All client and operational data is stored in Microsoft 365.
- Automated daily backups are maintained in secure cloud storage.
- Data restoration tests are conducted at least twice annually.

Client Communication

- Clients will be notified within 24 hours of any service disruption.
- Regular status updates will be provided until services are fully restored.

Disaster Recovery Procedures

Triggering Events

This plan is activated in the event of:

- Natural disaster (fire, flood, storm)
- Extended power or network outage
- Cybersecurity incident (ransomware, breach)
- Pandemic or public health crisis
- Major staff unavailability

Recovery Steps

- Assess Situation — Determine the type and extent of disruption.
- Activate BCDR Team — Managing Director authorizes response.
- Communicate — Notify employees, clients, and partners.
- Recover Systems — Restore data from backups, validate integrity.
- Resume Operations — Prioritize client-facing services.
- Post-Incident Review — Document incident and update policy.

Recovery Time Objectives (RTO)

Function	Target Recovery Time
Client Data Access	8 hours
Online Training Delivery	24 hours
Financial Systems	48 hours
Internal Communications	4 hours

Data Protection and Security

All data handling complies with GDPR and local privacy regulations.
MFA (Multi-Factor Authentication) and encryption are required for all systems.
Access to sensitive data is restricted to authorized personnel only.
Cybersecurity awareness training is conducted annually.

Testing and Maintenance

- BCDR tests are performed at least once per year.
- Lessons learned are documented and incorporated into future revisions.
- The Operations Manager ensures policy updates after any major incident or organizational change.

This policy will be regularly reviewed by Duncan Young Consulting Pty Ltd, and any necessary changes will be implemented by the DYC Management team. DYC reserves the right to update this policy at any time without notice, in order to address changed circumstances or legislation or improve business practices. You may obtain a copy of the current version of the Business Continuity and Disaster Recovery policy by contacting DYC.