Business Continuity and Disaster Recovery Policy

Gibble SaaS Platform

Prepared by: Gregory Ibbotson – G.I. IT Security

Version: 1.0

Leftorium Pty Ltd
Suite 204, 189E South Centre Road, Tullamarine VIC 3043
Email: info@gibble.com.au | Phone: (03) 9744 2887

ABN 65 7612 792
Trading as **Gibble** - *gibble.com.au*

Leftorium Pty Ltd (Trading as Gibble) Business Continuity and Disaster Recovery Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Business Continuity and Disaster Recovery Policy

Last updated: July 2025

1. Purpose

1.1 This Business Continuity and Disaster Recovery (BCDR) Policy ("Policy") outlines the procedures and measures implemented by Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), to ensure the continuity of critical operations and the rapid recovery of systems, data, and services following a disruption. This includes disruptions caused by cyberattacks, natural disasters, hardware failures, or human errors affecting our SaaS platforms for learning, payroll, student management, and human resources management.

1.2 The Policy integrates with our Security Policy (Section 5.5), Data Breach Response Plan, Information Security Incident Management Policy, and other policies, leveraging Adlumin Managed Detection and Response (MDR) services, Amazon Web Services (AWS), and Microsoft Entra infrastructure to ensure resilience.

1.3 We are committed to compliance with applicable data protection and cybersecurity standards, including:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth).
- EU General Data Protection Regulation 2016/679 (GDPR), Article 32.
- *Privacy Act 2020* (New Zealand), Information Privacy Principle (IPP) 5.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI).

1.4 For inquiries, contact our Business Continuity Officer at:

- **Email**: bcdr@gibble.com.au
- **Address**: Level 2, Suite 204, 189E South Centre Rd, Tullamarine VIC 3043, Australia
- **Phone**: +61 3 9744 2887

1.5 This Policy is reviewed annually or as needed to reflect changes in regulations, technology, or business operations. Updates are posted at www.gibble.com.au/bcdr.

2. Scope

2.1 This Policy applies to:

- All Gibble platforms, systems, and infrastructure, including those hosted on AWS (e.g., S3, RDS, EC2) and Microsoft Entra (e.g., Azure Blob Storage, Entra ID).
- Data processed through our Services, including personal information, customer data, and analytics data, as described in the Privacy Policy (Section 4).
- Critical business functions, such as platform operations, customer support, and data processing.
- Physical facilities, including Gibble's Tullamarine, VIC office, and third-party data centres.

- All users, including employees, contractors, customers, and vendors.

2.2 It covers disruptions such as cyberattacks, natural disasters (e.g., floods, earthquakes), power outages, hardware failures, and human errors, complementing the Data Breach Response Plan and Information Security Incident Management Policy.

3. Definitions

3.1 **Business Continuity (BC)**: Processes to ensure critical business functions continue during and after a disruption.
3.2 **Disaster Recovery (DR)**: Processes to restore systems, data, and infrastructure to normal operations after a disruption.
3.3 **Recovery Time Objective (RTO)**: The maximum acceptable downtime for a system or function before recovery.
3.4 **Recovery Point Objective (RPO)**: The maximum acceptable data loss, measured as the time between the last backup and the disruption.
3.5 **Critical Function**: A business process or system essential to Gibble's operations or customer commitments (e.g., platform availability, payroll processing).

4. BCDR Principles

4.1 **Resilience**: Design systems and processes to withstand disruptions and minimise downtime.
4.2 **Proactive Planning**: Identify critical functions and risks to ensure preparedness.
4.3 **Rapid Recovery**: Restore systems and data within defined RTOs and RPOs to meet customer expectations.
4.4 **Compliance**: Align with ISO 22301, ISO 27001, and data protection laws to protect data and ensure regulatory adherence.
4.5 **Continuous Improvement**: Regularly test and update BCDR plans based on lessons learned and evolving threats.

5. Critical Functions and RTO/RPO

5.1 **Critical Functions**:

- **Platform Operations**: Availability of learning, payroll, student management, and HR platforms.
- **Data Processing**: Processing of customer data, including payroll and student records.
- **Customer Support**: Access to support services via support@gibble.com.au.
- **Security Monitoring**: Real-time threat detection via Adlumin MDR.
- **Data Backup and Recovery**: Integrity and availability of backups in AWS S3 and Azure Blob Storage.

5.2 **RTO and RPO**:

Function	RTO	RPO	Rationale
Platform Operations	4 hours	15 minutes	Critical for customer SLAs; minimises operational impact.

Function	RTO	RPO	Rationale
Data Processing	8 hours	1 hour	Ensures timely payroll and student record processing.
Customer Support	12 hours	N/A	Maintains customer trust and communication.
Security Monitoring	2 hours	N/A	Ensures continuous threat detection via Adlumin MDR.
Data Backup and Recovery	12 hours	15 minutes	Aligns with backup frequency and data protection requirements.

6. Risk Assessment and Planning

6.1 **Risk Assessment**:

- Conduct annual risk assessments to identify potential disruptions (e.g., cyberattacks, natural disasters, vendor failures).
- Assess impact on critical functions, data, and customers, per the Security Policy (Section 4).
- Prioritise risks based on likelihood and severity, with mitigation plans documented.

6.2 **Business Impact Analysis (BIA)**:

- Identify dependencies (e.g., AWS, Microsoft Entra, Adlumin MDR).
- Determine acceptable downtime and data loss for each critical function.
- Update BIA annually or after significant changes (e.g., new platform features).

6.3 **BCDR Plan**:

- Maintains detailed recovery procedures for each critical function.
- Includes failover to alternate AWS regions (e.g., Asia Pacific, US West) or Azure data centres.
- Defines communication protocols for customers and stakeholders.

7. Backup and Storage

7.1 **Backup Procedures**:

- **Frequency**: Daily incremental backups and weekly full backups for all critical data, per the Security Policy (Section 5.5).
- **Storage**: Encrypted backups stored in AWS S3 and Azure Blob Storage with AES-256 encryption.
- **Retention**: 90 days for incremental backups, 1 year for full backups, per the Data Retention and Deletion Policy (Section 5).

- **Locations**: Multi-region storage in Australia, New Zealand, Canada, UK, Singapore, USA, and Japan.

7.2 **Backup Security**:

- Access restricted via AWS IAM and Entra ID with MFA, per the Access Control Policy (Section 5).
- Monitored by Adlumin MDR for unauthorised access attempts.
- Regular integrity checks to ensure backup reliability.

8. Incident Response Integration

8.1 **Incident Detection**:

- Leverage Adlumin MDR, AWS CloudTrail, and Microsoft Defender for Cloud for real-time detection of disruptions, per the Information Security Incident Management Policy (Section 6).
- Employees and vendors report incidents to bcdr@gibble.com.au within 1 hour.

8.2 **Incident Management**:

- Disruptions are classified per the Information Security Incident Management Policy (Section 7):
    - Low: Minimal impact (e.g., temporary network latency).
    - Medium: Limited impact (e.g., single platform outage).
    - High: Significant impact (e.g., multi-region outage).
    - Critical: Severe impact (e.g., data loss, platform unavailability).
- Data breaches are managed per the Data Breach Response Plan (Section 6).

8.3 **Containment and Recovery**:

- Immediate containment (e.g., isolate affected systems, failover to alternate regions) within 2 hours for critical incidents.
- Recovery follows RTO/RPO targets, using encrypted backups and verified procedures.
- Adlumin MDR supports containment and eradication of cyber threats.

9. BCDR Team

9.1 The BCDR Team includes:

- **Business Continuity Officer**: Leads BCDR planning and response (bcdr@gibble.com.au).
- **Security Officer**: Coordinates with Adlumin MDR for threat response.

- **IT Manager**: Manages technical recovery on AWS and Entra infrastructure.
- **Data Protection Officer (DPO)**: Ensures compliance with data protection laws.
- **Communications Lead**: Handles customer and stakeholder communications.
- **HR Representative**: Addresses employee-related impacts.

9.2 The BCDR Team reports to the CEO and is activated immediately upon disruption detection.

10. Recovery Procedures

10.1 **System Recovery**:

- Restore platforms from encrypted backups in AWS S3 or Azure Blob Storage.
- Failover to alternate AWS regions or Azure data centres if primary regions are unavailable.
- Verify system integrity before resuming operations, per the Information Security Incident Management Policy (Section 9).

10.2 **Data Recovery**:

- Restore data within RPO targets (e.g., 15 minutes for platform data).
- Ensure data integrity through checksum validation and Adlumin MDR scans.
- Notify customers of data restoration timelines, per SLAs.

10.3 **Customer Communication**:

- Notify customers of disruptions within 4 hours for high/critical incidents, via email or platform alerts.
- Provide recovery updates and support via support@gibble.com.au.

11. Testing and Training

11.1 **Testing**:

- Annual tabletop exercises simulate disruptions (e.g., ransomware, data centre failure).
- Biannual failover tests validate recovery to alternate AWS/Azure regions.
- Quarterly backup restoration tests ensure data integrity.

11.2 **Training**:

- Employees and contractors receive annual BCDR training, covering:
    - Incident reporting procedures.

    - Roles and responsibilities during disruptions.
    - Recovery processes for critical functions.
- Customers receive guidance on BCDR expectations during onboarding.

11.3 **Test Documentation**:

- Test results are documented, including recovery times, issues, and corrective actions.
- Lessons learned are incorporated into the BCDR Plan.

12. Compliance

12.1 This Policy aligns with:

- ISO 22301 (Business Continuity Management).
- ISO 27001 A.17 (Information Security Continuity).
- GDPR Article 32 (Security of Processing).
- APP 11.1 (Security of Personal Information).
- NIST 800-53 CP-2 (Contingency Planning).
- PDPA, CCPA/CPRA, and APPI continuity requirements.

12.2 AWS and Microsoft Entra compliance dashboards ensure adherence, with Adlumin MDR providing audit-ready logs.

13. Roles and Responsibilities

13.1 **Business Continuity Officer**:

- Develops and maintains the BCDR Plan.
- Coordinates testing and recovery efforts.
- Ensures compliance with regulations.

13.2 **Security Officer**:

- Monitors disruptions via Adlumin MDR.
- Supports containment and eradication of cyber incidents.

13.3 **IT Manager**:

- Executes backup and recovery procedures.

- Manages failover to alternate regions.

13.4 **Employees and Contractors**:

- Report disruptions within 1 hour to bcdr@gibble.com.au.
- Participate in BCDR training and tests.

13.5 **Vendors**:

- Support recovery efforts per the Vendor Management Policy (Section 7).
- Report disruptions within 24 hours.

14. Post-Incident Review

14.1 Conduct a review within 30 days of a disruption, documenting:

- Root cause and impact.
- Response and recovery effectiveness.
- Updates to the BCDR Plan or other policies (e.g., Security Policy).

14.2 Share findings with the CEO and customers (if applicable).

15. Contact Information

15.1 For BCDR inquiries or to report disruptions, contact:

- **Business Continuity Officer**: bcdr@gibble.com.au
- **Security Officer**: security@gibble.com.au
- **Data Protection Officer**: privacy@gibble.com.au
- **Phone**: +61 3 9744 2887

15.2 Complaints can be escalated to:

- **Australia**: Office of the Australian Information Commissioner, enquiries@oaic.gov.au, 1300 363 992.
- **New Zealand**: Office of the Privacy Commissioner, enquiries@privacy.org.nz.
- **EU**: Relevant supervisory authority (e.g., ICO in the UK).
- **Singapore**: Personal Data Protection Commission, info@pdpc.gov.sg.
- **USA**: Relevant state authority (e.g., California Attorney General).
- **Japan**: Personal Information Protection Commission, info@ppc.go.jp.