Change Management 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) Change Management Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Change Management Policy

Last updated: July 2025

1. Purpose

1.1 This Change Management Policy ("Policy") outlines the procedures for managing changes to the systems, platforms, applications, infrastructure, and processes of Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"). The Policy ensures that changes to our SaaS platforms for learning, payroll, student management, and human resources management are implemented in a controlled, secure, and compliant manner to minimize risks to operations, data, and customers.

1.2 The Policy integrates with our Security Policy (Section 6), Access Control Policy (Section 5), Information Security Incident Management Policy (Section 6), and other policies, leveraging Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to maintain system integrity and security during changes.

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

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APP 11.
- 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 Change Management Officer at:

- **Email**: change@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/change-management.

2. Scope

2.1 This Policy applies to:

- All changes to Gibble's platforms, systems, and infrastructure, including those hosted on AWS (e.g., S3, RDS, EC2), Microsoft Entra (e.g., Azure Blob Storage, Entra ID), and third-party systems (e.g., Salesforce, Stripe).
- Changes to software, hardware, configurations, databases, and operational processes.
- Data processed by Gibble, including personal information, customer data, and analytics data, as described in the Privacy Policy (Section 4).

- All personnel involved in changes, including employees, contractors (e.g., in Vietnam and the Philippines for Gibble platforms), and vendors.
- Physical infrastructure, including Gibble's Tullamarine, VIC office and data centres.

2.2 It complements the Security Policy (Section 6), Access Control Policy (Section 5), Vendor Management Policy (Section 5), and Business Continuity and Disaster Recovery Policy (Section 6) to ensure secure and stable change implementation.

3. Definitions

3.1 **Change**: Any modification to Gibble's systems, applications, infrastructure, or processes, including software updates, configuration changes, or new feature deployments.

3.2 **Change Request**: A formal proposal to implement a change, submitted for review and approval.

3.3 **Change Advisory Board (CAB)**: A group responsible for reviewing and approving changes.

3.4 **Emergency Change**: An urgent change required to address critical issues (e.g., security vulnerabilities, system outages).

4. Change Management Principles

4.1 **Controlled Implementation**: Changes are planned, tested, and documented to minimize risks to system stability and data security.

4.2 **Risk Assessment**: All changes are evaluated for potential impacts on operations, security, and compliance.

4.3 **Accountability**: Changes are tracked, logged, and auditable to ensure traceability.

4.4 **Minimization of Disruption**: Changes are scheduled to minimize impact on customers and critical functions, per the Business Continuity and Disaster Recovery Policy (Section 5).

4.5 **Compliance**: Changes adhere to data protection and cybersecurity standards, including ISO 27001 and GDPR.

5. Change Management Process

5.1 **Change Identification**:

- Changes may be initiated to address:
    - System updates (e.g., software patches, feature enhancements).
    - Security vulnerabilities, per the Information Security Incident Management Policy (Section 7).
    - Customer requirements or contractual obligations.

    - Performance improvements or infrastructure upgrades.

- Changes are identified by employees, contractors, vendors, or customers and submitted to change@gibble.com.au.

5.2 **Change Request Submission**:

- Change requests include:
    - Description of the change and purpose.
    - Affected systems, data, or processes.
    - Risk assessment and potential impacts.
    - Proposed implementation plan and timeline.
- Requests are submitted via a secure change management system (e.g., AWS Service Catalogue, internal ticketing system).

5.3 **Change Review and Approval**:

- The Change Advisory Board (CAB), comprising the Change Management Officer, Security Officer, IT Manager, and Data Protection Officer (DPO), reviews requests.
- Criteria for approval include:
    - Alignment with business objectives and customer SLAs.
    - Security and compliance risks, per the Security Policy (Section 6).
    - Impact on critical functions, per the Business Continuity and Disaster Recovery Policy (Section 5).
- Emergency changes bypass standard review but require post-implementation approval within 24 hours.

5.4 **Testing and Validation**:

- Changes are tested in a non-production environment (e.g., AWS staging environment, Azure sandbox).
- Tests verify functionality, security (e.g., penetration testing), and data integrity, per the Encryption Policy (Section 5).
- Adlumin MDR monitors test environments for anomalies.

5.5 **Implementation**:

- Approved changes are implemented by the IT Manager or authorized contractors (e.g., Gibble team in Vietnam/Philippines).
- Implementation follows a rollback plan to revert changes if issues arise.
- Changes are scheduled during low-impact windows, with customer notification if downtime is expected.

5.6 **Post-Implementation Review**:

- Within 48 hours, the CAB reviews the change outcome, including:
    - Success or failure of the change.
    - Any incidents triggered, per the Information Security Incident Management Policy (Section 7).
    - Updates to documentation or processes.
- Results are logged in AWS CloudTrail and Microsoft Defender for Cloud.

6. Change Types

6.1 **Standard Changes**:

- Pre-approved, low-risk changes (e.g., routine software updates, configuration tweaks).
- Follow automated workflows in AWS or Entra systems.

6.2 **Normal Changes**:

- Require CAB approval due to moderate risk or impact (e.g., new feature deployments, database schema changes).
- Follow the full change management process (Section 5).

6.3 **Emergency Changes**:

- Address critical issues (e.g., zero-day vulnerabilities, system outages).
- Implemented immediately with Security Officer approval, followed by CAB review within 24 hours.
- Monitored by Adlumin MDR for security impacts.

7. Security and Compliance

7.1 **Security Measures**:

- Changes are implemented using encrypted channels (TLS 1.3) and secure systems (AES-256), per the Encryption Policy (Section 5).
- Access to change environments is restricted via AWS IAM and Entra ID with MFA, per the Access Control Policy (Section 5).
- Adlumin MDR monitors changes for unauthorized access or anomalies.

7.2 **Compliance**:

- Changes comply with ISO 27001 A.12.1.2 (Change Management), GDPR Article 32, and APP 11.
- Data subject rights (e.g., access, deletion) are maintained during changes, per the Data Subject Rights Policy (Section 6).

- Vendor-related changes comply with Data Protection Agreements (DPAs), per the Vendor Management Policy (Section 5).

7.3 **Risk Mitigation**:

- Risk assessments evaluate impacts on data security, system availability, and customer SLAs.
- Backup and rollback plans are prepared before implementation, per the Business Continuity and Disaster Recovery Policy (Section 7).

8. Monitoring and Auditing

8.1 **Monitoring**:

- Adlumin MDR monitors change activities for security risks (e.g., unauthorized configuration changes).
- AWS CloudTrail and Microsoft Defender for Cloud log all change-related events.

8.2 **Auditing**:

- Quarterly audits verify compliance with this Policy, including change documentation and approval processes.
- Annual ISO 27001 and SOC 2 Type II audits include change management reviews.
- Audit reports are available to customers upon request at security@gibble.com.au.

9. Roles and Responsibilities

9.1 **Change Management Officer**:

- Oversees the change management process and chairs the CAB.
- Ensures documentation and compliance with this Policy.
- Coordinates post-implementation reviews.

9.2 **Security Officer**:

- Assesses security risks of proposed changes.
- Monitors change implementation with Adlumin MDR.
- Approves emergency changes.

9.3 **IT Manager**:

- Implements and tests changes in AWS and Entra systems.
- Maintains rollback plans and backup integrity.
- Documents change outcomes.

9.4 **Data Protection Officer (DPO)**:

- Ensures changes comply with data protection laws.
- Addresses data subject rights concerns during changes (privacy@gibble.com.au).

9.5 **Employees and Contractors**:

- Submit change requests and adhere to this Policy.
- Report issues during change implementation to change@gibble.com.au.
- Participate in change-related training, per the Employee and Contractor Security Policy (Section 7).

9.6 **Vendors**:

- Comply with change management requirements in DPAs, per the Vendor Management Policy (Section 5).
- Notify Gibble of vendor-initiated changes affecting services.

10. Training

10.1 Employees and contractors, including those in Vietnam and the Philippines, receive annual training on:

- Change management procedures and risk assessment.
- Secure implementation of changes.
- Reporting change-related incidents.

10.2 Customers receive guidance on change impacts during onboarding or major updates, per the Acceptable Use Policy (Section 5).

11. Violations

11.1 Violations of this Policy (e.g., unauthorized changes, bypassing CAB approval) may result in:

- Disciplinary action for employees or contractors, per the Employee and Contractor Security Policy (Section 12).
- Immediate suspension of access, per the Access Control Policy (Section 12).
- Contractual penalties for vendors, per the Vendor Management Policy (Section 12).
- Reporting to regulators if the violation constitutes a data breach, per the Data Breach Response Plan (Section 8).

11.2 Violations are investigated by the Security Officer with Adlumin MDR support, with findings escalated to the CEO or Data Breach Response Team as needed.

12. Contact Information

12.1 For change management inquiries or to report issues, contact:

- **Change Management Officer**: change@gibble.com.au
- **Security Officer**: security@gibble.com.au
- **Data Protection Officer**: privacy@gibble.com.au
- **Phone**: +61 3 9744 2887

12.2 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.