Security 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) Security Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Security Policy

Last updated: July 2025

1. Introduction

1.1 This Security Policy outlines the technical and organisational measures implemented by Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), to protect personal information, systems, and assets across our SaaS platforms for learning, payroll, student management, and human resources management. It applies to all Gibble infrastructure, including cloud environments hosted on Amazon Web Services (AWS) and Microsoft Entra, and incorporates Managed Detection and Response (MDR) services provided by Adlumin.

1.2 We are committed to maintaining the highest security standards, aligning with ISO 27001, and complying with applicable data protection and cybersecurity regulations, including:

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

1.3 For inquiries, contact our Security Officer at:

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

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

2. Scope

2.1 This Security Policy applies to:

- All Gibble platforms, applications, and services.
- Infrastructure hosted on AWS and Microsoft Entra.
- Data processed on behalf of customers, end users, and data subjects.
- Internal systems, employee devices, and third-party integrations.
- MDR services provided by Adlumin for threat detection and response.

2.2 It covers the confidentiality, integrity, and availability of personal information, customer data, and Gibble's IT systems, as outlined in our Privacy Policy at www.gibble.com.au/privacy.

3. Security Framework and Compliance

3.1 Gibble aligns its security practices with ISO 27001, implementing an Information Security Management System (ISMS) to ensure consistent risk management and continuous improvement.

3.2 AWS Compliance: Our AWS infrastructure adheres to 143 security standards and certifications, including:

- ISO 27001, ISO 27017, ISO 27018.
- SOC 1, SOC 2, SOC 3.
- PCI-DSS, HIPAA/HITECH, FedRAMP.
- GDPR, NIST 800-171, FIPS 140-2.
- Australian Government's Hosting Certification Framework (HCF) Strategic Hosting Provider certification.

3.3 Microsoft Entra Compliance: Our Microsoft Entra environment complies with:

- ISO 27001, ISO 27018.
- SOC 1, SOC 2, SOC 3.
- GDPR, NIST 800-53, CSA STAR.
- Microsoft Cloud Security Benchmark (MCSB) controls.

3.4 Adlumin MDR Compliance: Adlumin's MDR services enhance our security posture with compliance to:

- NIST Cybersecurity Framework.
- SOC 2 Type II.
- GDPR and CCPA requirements for incident response and data protection.

3.5 Gibble ensures compliance with regional regulations through regular audits, risk assessments, and third-party certifications, supporting customers in meeting their compliance obligations.

4. Infrastructure Security

4.1 AWS Infrastructure:

- **Data Centres**: Hosted in secure AWS regions (Australia, New Zealand, Canada, UK, Singapore, USA, Japan) with 24/7 monitoring, physical access controls, and environmental safeguards.
- **Encryption**: AES-256 for data at rest, TLS 1.3 for data in transit.
- **Network Security**: Virtual Private Clouds (VPCs), AWS Web Application Firewall (WAF), and AWS Shield for DDoS protection.
- **Access Controls**: AWS Identity and Access Management (IAM) with least privilege principles and multi-factor authentication (MFA).

- **Monitoring**: AWS CloudTrail and Amazon GuardDuty for real-time threat detection, integrated with Adlumin MDR.

4.2 Microsoft Entra Infrastructure:

- **Identity Management**: Entra ID enforces role-based access control (RBAC), MFA, and conditional access policies.
- **Security Monitoring**: Microsoft Defender for Cloud provides threat detection, compliance reporting, and integration with Adlumin MDR for unified monitoring.
- **Encryption**: Data encrypted using Azure Key Vault and Microsoft-managed keys.
- **Compliance**: Aligns with MCSB for regulatory compliance tracking.

4.3 Adlumin MDR Services:

- **Threat Detection**: 24/7 monitoring of Gibble infrastructure using AI-driven analytics and behavioural analysis to detect threats (e.g., malware, ransomware, insider threats).
- **Incident Response**: Automated and manual response actions, including threat containment, remediation, and forensic analysis.
- **Log Management**: Centralised logging and analysis across AWS, Entra, and on-premises systems for real-time visibility.
- **Compliance Reporting**: Automated reports for GDPR, APPs, and other standards, ensuring audit readiness.

5. Data Security Measures

5.1 Data Classification: All data (e.g., personal information, customer data, analytics) is classified based on sensitivity (public, internal, confidential, restricted).

5.2 Encryption:

- Data at rest: AES-256 encryption across AWS S3, RDS, and Azure Blob Storage.
- Data in transit: TLS 1.3 for all communications, including API calls and platform access.
- Biometric data (e.g., fingerprints for time tracking): Encrypted and stored separately with restricted access.

5.3 Access Controls:

- Role-based access enforced via AWS IAM and Entra ID.
- MFA required for all privileged accounts and sensitive operations.
- Session timeouts and automatic logouts for inactive users.

5.4 Data Segregation: Customer data is logically separated using tenant-specific databases and VPCs to prevent unauthorised access.

5.5 Backup and Recovery:

- Automated backups stored in encrypted AWS S3 and Azure Blob Storage.
- Regular testing of disaster recovery processes to ensure data availability.
- Retention policies align with customer contracts and legal requirements (e.g., 7 years for tax-related data in Australia).

6. Platform Security

6.1 Application Security:

- Secure Software Development Lifecycle (SDLC) with code reviews and static/dynamic application security testing (SAST/DAST).
- Regular penetration testing by third-party providers to identify vulnerabilities.
- OWASP Top Ten compliance for web application security.

6.2 API Security:

- APIs secured with OAuth 2.0, API keys, and rate limiting.
- Encrypted data transmission via TLS 1.3.
- Monitoring for suspicious API activity via Adlumin MDR.

6.3 End-User Security:

- Secure authentication via Entra ID with single sign-on (SSO) and MFA.
- Session management with secure cookies and token-based authentication.
- User access logs audited for compliance and security monitoring.

7. Managed Detection and Response (Adlumin)

7.1 Deployment: Adlumin MDR is deployed across all Gibble infrastructure, including AWS, Microsoft Entra, and on-premises systems, providing:

- Real-time threat detection using machine learning and behavioural analytics.
- Automated incident response to mitigate threats (e.g., isolating compromised systems).
- 24/7 Security Operations Center (SOC) support for incident investigation and remediation.

7.2 Integration:

- Unified visibility with AWS CloudTrail, GuardDuty, and Microsoft Defender for Cloud.
- Centralised logging and correlation of security events across all platforms.
- Proactive threat hunting to identify advanced persistent threats (APTs).

7.3 Incident Response:

- Adlumin follows a defined incident response plan, including:
    - Detection and classification within minutes.
    - Containment and eradication within hours.
    - Post-incident analysis and reporting within 72 hours (per GDPR Article 33).
- Customers are notified of breaches as required by law (e.g., within 72 hours under GDPR).

8. Employee and Contractor Security

8.1 Training: All employees and contractors undergo mandatory annual training on:

- Data protection and cybersecurity best practices.
- Phishing and social engineering awareness.
- Compliance with ISO 27001 and regional regulations.

8.2 Access Management:

- Employees and contractors access systems via Entra ID with MFA and least privilege principles.
- Access is revoked immediately upon termination or role change.

8.3 Confidentiality: All personnel sign confidentiality agreements, with additional security obligations for contractors in Vietnam and the Philippines (e.g., Gibble platforms).

9. Third-Party Security

9.1 Vendor Management:

- Third-party providers (e.g., AWS, Microsoft, Adlumin, Stripe, Salesforce) are vetted for ISO 27001 or SOC 2 compliance.
- Contracts include data protection agreements (DPAs) compliant with GDPR and APPs.

9.2 Data Sharing:

- Data shared with third parties (e.g., hosting providers, payment gateways) is encrypted and governed by strict access controls.
- International transfers use Standard Contractual Clauses (SCCs) for GDPR-covered data.

10. Incident Response and Data Breach Management

10.1 Data Breach Response Plan:

- Aligns with APP 11, GDPR Article 33, and New Zealand's mandatory breach notification requirements.
- Steps include:
    - Identification and containment within 24 hours.
    - Assessment and notification to affected parties within 72 hours (if required).
    - Root cause analysis and remediation to prevent recurrence.

10.2 Adlumin MDR Role:

- Real-time monitoring and automated response to contain breaches.
- Detailed incident reports for customers and regulators.

10.3 Customer Notification:

- Customers are notified of breaches impacting their data subjects, with details on affected data and mitigation steps.
- Data subjects are informed via customers, as per our Privacy Policy.

11. Physical Security

11.1 Office Security:

- Biometric locks, surveillance systems, and visitor access controls at our Tullamarine, VIC office.
- Secure storage for hard-copy records, with verified destruction via certified providers.

11.2 Data Centres:

- AWS and Microsoft data centres employ 24/7 security, biometric access, and environmental controls (e.g., fire suppression, power redundancy).

12. Compliance and Auditing

12.1 Internal Audits:

- Quarterly security audits to assess compliance with ISO 27001 and regional regulations.
- Annual penetration testing and vulnerability scans.

12.2 External Audits:

- Third-party audits for SOC 2 Type II and ISO 27001 certification.
- Compliance reports available to customers upon request.

12.3 Regulatory Compliance:

- Regular monitoring of AWS and Microsoft Entra compliance dashboards for adherence to GDPR, CCPA, PDPA, and APPI.
- Adlumin MDR provides automated compliance reporting for audit trails.

13. Customer Responsibilities

13.1 Customers must:

- Ensure their use of Gibble platforms complies with applicable laws.
- Obtain consents for data collection and processing, as outlined in our Privacy Policy.
- Maintain accurate and up-to-date data entered into our platforms.

13.2 Customers can request security documentation or audit reports via security@gibble.com.au.

14. Contact Us

14.1 For security-related inquiries or to report a security incident, contact our Security Officer at security@gibble.com.au.

14.2 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.