Vendor 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) Vendor Management Policy

Last updated: July 2025

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	Definitions	4
4.	Vendor Management Principles	4
5.	Vendor Selection and Onboarding	4
6.	Vendor Monitoring and Performance	5
7.	Vendor Risk Management	6
8.	Vendor Termination	6
9.	Roles and Responsibilities	7
10.	Compliance	8
11.	Training	8
12.	Violations	8
13.	Contact Information	8

Leftorium Pty Ltd (Trading as Gibble) Vendor Management Policy

Last updated: July 2025

1. Purpose

1.1 This Vendor Management Policy ("Policy") outlines the processes and requirements for selecting, onboarding, monitoring, and managing third-party vendors engaged by Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), to support our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures that vendors meet Gibble's privacy, security, and compliance standards to protect personal information, customer data, and our systems.

1.2 The Policy aligns with our Security Policy (Section 9), Privacy Policy (Section 10), and Data Breach Response Plan, leveraging Adlumin Managed Detection and Response (MDR) services, Amazon Web Services (AWS), and Microsoft Entra infrastructure.

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).
- EU General Data Protection Regulation 2016/679 (GDPR), Article 28.
- *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 Vendor Management Officer at:

- **Email**: vendors@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/vendor-management.

2. Scope

2.1 This Policy applies to:

- All third-party vendors providing services to Gibble, including cloud hosting (e.g., AWS, Microsoft), security (e.g., Adlumin MDR), payment processing (e.g., Stripe), CRM (e.g., Salesforce), and development/support contractors (e.g., in Vietnam and the Philippines for Gibble platforms).
- Data processed by vendors, including personal information, customer data, and analytics data, as described in the Privacy Policy (Section 4).
- Vendor interactions with Gibble's platforms, systems, and infrastructure hosted on AWS and Microsoft Entra.

2.2 It complements the Security Policy (Section 9), Privacy Policy (Section 10), Data Breach Response Plan (Section 12), Acceptable Use Policy (Section 8), and Access Control Policy (Section 6).

3. Definitions

3.1 **Vendor**: Any third-party organisation or individual providing services to Gibble, including cloud providers, software vendors, contractors, and professional services (e.g., legal, financial advisors).

3.2 **Personal Information**: Information relating to an identified or identifiable individual, as defined in the Privacy Policy (Section 4).

3.3 **Data Protection Agreement (DPA)**: A legally binding contract ensuring vendors comply with data protection laws when processing Gibble's data.

3.4 **Standard Contractual Clauses (SCCs)**: Agreements ensuring compliance with GDPR for international data transfers.

4. Vendor Management Principles

4.1 **Due Diligence**: Vendors are selected based on their ability to meet Gibble's security, privacy, and compliance standards

4.2 **Contractual Obligations**: Vendors must sign DPAs and adhere to Gibble's policies, including the Security Policy and Acceptable Use Policy.

4.3 **Continuous Monitoring**: Vendor performance and compliance are regularly assessed to ensure ongoing adherence to standards.

4.4 **Risk Management**: Vendor-related risks are identified, mitigated, and monitored to protect Gibble's data and systems.

4.5 **Accountability**: Vendors are accountable for breaches or non-compliance, with clear escalation and remediation processes.

5. Vendor Selection and Onboarding

5.1 **Due Diligence**:

- Vendors are evaluated based on:

    - Security certifications (e.g., ISO 27001, SOC 2 Type II).
    - Compliance with GDPR, APPs, PDPA, CCPA, APPI, and other relevant laws.
    - Financial stability and reputation.
    - Technical capabilities (e.g., encryption, access controls).
- Documentation reviewed includes security policies, audit reports, and compliance certifications.
- Vendors handling sensitive data (e.g., biometric, payroll) undergo enhanced scrutiny.

5.2 **Data Protection Agreements (DPAs)**:

- Vendors sign DPAs outlining:
    - Data processing scope, purpose, and duration.
    - Security obligations (e.g., AES-256 encryption, TLS 1.3, MFA).
    - Breach notification requirements (within 24 hours, per Data Breach Response Plan, Section 12).
    - Sub-processor management and approval processes.
    - Compliance with GDPR Article 28, APP 8, and other laws.
- SCCs are included for international data transfers (Privacy Policy, Section 13).

5.3 **Onboarding**:

- Vendors receive Gibble's Security Policy, Acceptable Use Policy, and Access Control Policy.
- Access to systems is granted via AWS IAM or Microsoft Entra, with role-based access control (RBAC) and MFA, as per the Access Control Policy (Section 5).
- Contractors (e.g., in Vietnam, Philippines for Gibble platforms) sign confidentiality agreements and undergo security training.

6. Vendor Monitoring and Performance

6.1 **Continuous Monitoring**:

- Adlumin MDR monitors vendor-related activities (e.g., API access, data transfers) for anomalies or unauthorised access.
- AWS CloudTrail and Microsoft Defender for Cloud log vendor interactions with Gibble's infrastructure.
- Vendors provide regular compliance reports (e.g., SOC 2, ISO 27001 audit results).

6.2 **Performance Reviews**:

- Annual vendor reviews assess:

    - Compliance with DPAs and Gibble policies.
    - Security posture (e.g., patch management, vulnerability scans).
    - Incident response performance (e.g., timeliness of breach notifications).
- Reviews are conducted by the Vendor Management Officer and Security Officer.

6.3 **Audits**:

- Vendors are subject to annual third-party audits, with results shared with Gibble.
- Gibble conducts on-site or remote audits for high-risk vendors (e.g., those handling biometric data).
- Audit findings are documented and addressed within 30 days.

7. Vendor Risk Management

7.1 **Risk Assessment**:

- Vendors are classified by risk level (low, medium, high) based on:
    - Type of data processed (e.g., personal, sensitive, biometric).
    - Access level to Gibble systems (e.g., full, restricted).
    - Geographic location (e.g., jurisdictions with weaker data protection laws).
- High-risk vendors (e.g., AWS, Adlumin) undergo enhanced due diligence and monitoring.

7.2 **Mitigation Measures**:

- Encryption and access controls enforced via AWS IAM and Entra ID.
- Regular penetration testing of vendor integrations, as per the Security Policy (Section 6).
- Contractual clauses for immediate termination if vendors fail to meet security standards.

7.3 **Incident Management**:

- Vendors must report security incidents or breaches within 24 hours to security@gibble.com.au, per the Data Breach Response Plan (Section 12).
- Adlumin MDR provides forensic analysis for vendor-related incidents.

8. Vendor Termination

8.1 **Termination Process**:

- Upon contract termination, vendor access is revoked immediately via AWS IAM and Entra ID, as per the Access Control Policy (Section 6.3).

- Vendors must return or delete all Gibble data, as per the Data Retention and Deletion Policy (Section 6).
- Deletion is verified through audit logs and vendor certifications.

8.2 **Data Handling**:

- Vendors confirm data deletion in writing within 30 days of termination.
- Residual data in backups is deleted per retention schedules (e.g., 90 days for incremental backups).

8.3 **Post-Termination Review**:

- The Vendor Management Officer conducts a review to ensure no data or access remains with the vendor.
- Findings are documented and retained for audit purposes.

9. Roles and Responsibilities

9.1 **Vendor Management Officer**:

- Oversees vendor selection, onboarding, and monitoring.
- Maintains a vendor registry with risk levels and compliance status.
- Coordinates audits and performance reviews.

9.2 **Security Officer**:

- Ensures vendor compliance with security requirements (e.g., encryption, MFA).
- Monitors vendor activity via Adlumin MDR and AWS/Microsoft tools.
- Investigates vendor-related incidents.

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

- Ensures vendor compliance with data protection laws (e.g., GDPR, APPs).
- Reviews DPAs and SCCs for legal compliance.
- Handles data subject inquiries involving vendors (privacy@gibble.com.au).

9.4 **Vendors**:

- Comply with Gibble's policies and DPAs.
- Report incidents within 24 hours and cooperate with investigations.
- Maintain security certifications and provide audit reports.

10. Compliance

10.1 This Policy aligns with:

- ISO 27001 A.15 (Supplier Relationships).
- GDPR Article 28 (Processor Obligations).
- APP 8 (Cross-Border Disclosure).
- NIST 800-53 SA-9 (External Information System Services).
- PDPA, CCPA/CPRA, and APPI vendor management requirements.

10.2 AWS and Microsoft Entra compliance dashboards track vendor adherence to these standards, with Adlumin MDR providing audit-ready logs.

11. Training

11.1 Employees involved in vendor management receive annual training on:

- Vendor due diligence and risk assessment.
- DPA and SCC requirements.
- Incident reporting and escalation procedures.

11.2 Vendors receive onboarding briefings on Gibble's Security Policy, Acceptable Use Policy, and Access Control Policy.

12. Violations

12.1 Vendor non-compliance (e.g., failure to report breaches, inadequate security) may result in:

- Immediate contract termination.
- Suspension of data processing activities.
- Legal action for damages caused by non-compliance.
- Reporting to regulators if the violation constitutes a data breach, per the Data Breach Response Plan (Section 8).

12.2 Violations are investigated by the Security Officer, with support from Adlumin MDR and the Data Breach Response Team.

13. Contact Information

13.1 For vendor-related inquiries or to report issues, contact:

Last updated: July 2025

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

13.2 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.