

Employee and Contractor 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) Employee and Contractor Security Policy

Last updated: July 2025

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	Definitions	4
4.	Security Principles	4
5.	Security Responsibilities	4
6.	Confidentiality Agreements	5
7.	Training and Awareness	6
8.	Monitoring and Auditing	6
9.	Incident Reporting and Response	7
10.	Termination and Offboarding	7
11.	Compliance	7
12.	Violations	8
13.	Roles and Responsibilities	8
14.	Contact Information	9

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

1. Purpose

1.1 This Employee and Contractor Security Policy ("Policy") outlines the security responsibilities and obligations of employees and contractors working for or on behalf of Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"). The Policy ensures the protection of Gibble's systems, platforms, and data, including personal information, customer data, and sensitive information processed through our SaaS platforms for learning, payroll, student management, and human resources management.

1.2 The Policy integrates with our Security Policy (Section 8), Privacy Policy (Section 19), Access Control Policy (Section 5), Acceptable Use Policy (Section 5), and other policies, leveraging Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to maintain a secure environment.

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 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

1.5 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/employee-security.

2. Scope

2.1 This Policy applies to:

- All employees and contractors of Gibble, including those in Australia, Vietnam, and the Philippines (e.g., supporting Gibble platforms).
- Gibble's 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 by Gibble, including personal information (e.g., names, contact details, biometric data), customer data, and analytics data, as described in the Privacy Policy (Section 4).

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

- Physical facilities, including Gibble's Tullamarine, VIC office, and third-party data centres.

2.2 It complements the Security Policy (Section 8), Access Control Policy (Section 5), Acceptable Use Policy (Section 5), and other policies to ensure a cohesive security framework.

3. Definitions

3.1 **Employee:** An individual employed by Gibble under a contract of employment.

3.2 **Contractor:** An individual or entity engaged by Gibble under a contract for services, including developers and support staff in Vietnam and the Philippines for Gibble platforms.

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

3.4 **Sensitive Data:** Data requiring heightened protection, such as biometric data, payroll records, or customer billing information.

4. Security Principles

4.1 **Confidentiality:** Employees and contractors must protect sensitive data from unauthorised access or disclosure.

4.2 **Least Privilege:** Access is granted only to the extent necessary for job functions, per the Access Control Policy (Section 4).

4.3 **Accountability:** All actions are logged and auditable to ensure traceability.

4.4 **Compliance:** Employees and contractors must comply with Gibble's policies and applicable data protection laws.

4.5 **Proactive Security:** Employees and contractors are trained to recognise and mitigate security risks.

5. Security Responsibilities

5.1 **General Obligations:**

- Comply with all Gibble policies, including the Acceptable Use Policy (Section 5), Access Control Policy (Section 5), and Encryption Policy (Section 5).
- Protect confidential and sensitive data, including customer data, biometric data, and intellectual property.
- Use only company-issued or approved devices and accounts for work-related activities.
- Report suspected security incidents or policy violations to security@gibble.com.au within 1 hour, per the Information Security Incident Management Policy (Section 6).

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

5.2 Access Management:

- Use strong passwords (minimum 12 characters, including uppercase, lowercase, numbers, and special characters) and enable multi-factor authentication (MFA) for all accounts, per the Access Control Policy (Section 5.1).
- Do not share credentials or allow unauthorised access to Gibble systems.
- Request access through the IT Manager, with approval from the Security Officer, per the Access Control Policy (Section 6.1).
- Immediately report lost or compromised credentials to security@gibble.com.au.

5.3 Data Handling:

- Process personal information only for authorised purposes, as per the Privacy Policy (Section 3).
- Encrypt sensitive data using AES-256 for storage and TLS 1.3 for transmission, per the Encryption Policy (Section 5).
- Do not store sensitive data on unapproved devices or unencrypted media.
- Follow the Data Retention and Deletion Policy (Section 6) for data disposal.

5.4 Device Security:

- Use company-issued devices with endpoint protection (e.g., antivirus, firewalls) managed by Microsoft Intune, per the Security Policy (Section 5.3).
- Ensure devices are updated with the latest security patches.
- Do not install unapproved software or use jailbroken devices.
- Report lost or stolen devices to security@gibble.com.au immediately.

5.5 Physical Security:

- Secure physical records (e.g., hard-copy files) in locked cabinets at Gibble's Tullamarine office, per the Access Control Policy (Section 7).
- Use biometric access controls for office entry and report unauthorised access attempts.
- Do not leave sensitive documents unattended.

6. Confidentiality Agreements

6.1 All employees and contractors must sign confidentiality agreements as part of their onboarding process, committing to:

- Protect Gibble's and customers' confidential information.

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

- Not disclose sensitive data without authorisation.
- Return or destroy data upon termination, per the Data Retention and Deletion Policy (Section 6).

6.2 Contractors in Vietnam and the Philippines supporting Gibble platforms sign additional security clauses specific to their roles.

7. Training and Awareness

7.1 Mandatory Training:

- All employees and contractors complete annual security training, covering:
 - Recognising phishing, malware, and social engineering attacks.
 - Proper data handling and encryption practices.
 - Incident reporting procedures.
 - Compliance with Gibble's policies and data protection laws.
- Training is delivered via online modules and in-person sessions, tracked for completion.

7.2 Onboarding:

- New employees and contractors receive security training within their first week.
- Contractors in Vietnam and the Philippines receive role-specific training for Gibble platforms.

7.3 Ongoing Awareness:

- Monthly security bulletins and simulated phishing exercises to reinforce awareness.
- Updates on emerging threats shared via internal communications.

8. Monitoring and Auditing

8.1 Monitoring:

- Adlumin MDR monitors employee and contractor activities for unauthorised access or anomalies, per the Information Security Incident Management Policy (Section 6).
- AWS CloudTrail and Microsoft Defender for Cloud log all system interactions, per the Access Control Policy (Section 8).

8.2 Auditing:

- Quarterly audits verify compliance with this Policy, including access reviews and training completion.
- Annual ISO 27001 and SOC 2 Type II audits include employee and contractor security practices.

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

- Audit reports are available to customers upon request at security@gibble.com.au.

9. Incident Reporting and Response

9.1 Reporting:

- Employees and contractors must report suspected security incidents (e.g., unauthorised access, data loss) to security@gibble.com.au within 1 hour, per the Information Security Incident Management Policy (Section 6).
- Reports include incident details, affected systems, and potential impacts.

9.2 Response:

- The Security Officer investigates incidents with Adlumin MDR support, per the Information Security Incident Management Policy (Section 7).
- Incidents involving personal information are escalated to the Data Breach Response Team, per the Data Breach Response Plan (Section 5).

10. Termination and Offboarding

10.1 Access Revocation:

- Upon termination, access to Gibble systems is revoked immediately via AWS IAM and Entra ID, per the Access Control Policy (Section 6.3).
- Company-issued devices are wiped or returned, per the Data Retention and Deletion Policy (Section 6).

10.2 Data Handling:

- Employees and contractors return or destroy all Gibble data, with verification by the IT Manager.
- Contractors in Vietnam and the Philippines confirm data deletion for Gibble platforms.

10.3 Post-Termination Audit:

- The Security Officer conducts a review to ensure no residual access or data remains.
- Findings are documented for compliance audits.

11. Compliance

11.1 This Policy aligns with:

- ISO 27001 A.7 (Human Resource Security).
- GDPR Article 32 (Security of Processing).

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

- APP 11 (Security of Personal Information).
- NIST 800-53 PS-3 (Personnel Security).
- PDPA, CCPA/CPRA, and APPI security requirements.

11.2 AWS and Entra compliance dashboards, supported by Adlumin MDR logs, ensure adherence to these standards.

12. Violations

12.1 Violations of this Policy (e.g., sharing credentials, failing to report incidents) may result in:

- Disciplinary action, up to and including termination of employment or contracts.
- Immediate suspension of access, per the Access Control Policy (Section 12).
- Legal action for serious violations causing harm to Gibble or customers.
- 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 Adlumin MDR support, with findings escalated to the CEO or Data Breach Response Team as needed.

13. Roles and Responsibilities

13.1 **Security Officer:**

- Oversees policy implementation and compliance.
- Investigates violations and incidents.
- Coordinates security training and audits.

13.2 **HR Manager:**

- Ensures confidentiality agreements are signed.
- Manages onboarding and offboarding processes.
- Tracks training completion.

13.3 **IT Manager:**

- Configures and revokes access via AWS IAM and Entra ID.
- Manages device security and data deletion during offboarding.

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

Leftorium Pty Ltd (Trading as Gibble) Employee and Contractor Security Policy

Last updated: July 2025

- Ensures compliance with data protection laws.
- Addresses data subject inquiries involving employees or contractors (privacy@gibble.com.au).

13.5 Employees and Contractors:

- Comply with this Policy and report violations or incidents.
- Complete mandatory training and protect Gibble's systems and data.

14. Contact Information

14.1 For inquiries or to report violations, contact:

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

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.