

Physical 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) Physical Security Policy

Last updated: July 2025

Table of Contents

1.	PURPOSE	3
2.	SCOPE	3
3.	DEFINITIONS	4
4.	PHYSICAL SECURITY PRINCIPLES	4
5.	PHYSICAL SECURITY CONTROLS	4
6.	PROCEDURES	5
7.	MONITORING AND AUDITING	6
8.	ROLES AND RESPONSIBILITIES	6
9.	TRAINING	7
10.	COMPLIANCE	7
11.	VIOLATIONS	7
12.	CONTACT INFORMATION	7

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

1. Purpose

1.1 This Physical Security Policy ("Policy") outlines the standards and procedures for protecting the physical assets, facilities, and personnel of Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), including our office premises and any physical media containing sensitive data. The Policy ensures the security of our SaaS platforms for learning, payroll, student management, and human resources management by preventing unauthorised physical access that could compromise systems, data, or operations.

1.2 The Policy integrates with our Security Policy (Section 11), Access Control Policy (Section 7), Employee and Contractor Security Policy (Section 5), and other policies, leveraging surveillance systems and biometric locks for physical security.

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 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/policies

2. Scope

2.1 This Policy applies to:

- Gibble's physical facilities, including the Tullamarine, VIC office at Level 2, Suite 204, 189E South Centre Rd, Tullamarine VIC 3043, Australia, and any remote or third-party sites used for operations (e.g., data centres for AWS and Microsoft Entra).
- All physical assets, including servers, storage devices, hard-copy records, and other media containing personal information, customer data, or sensitive data, as described in the Privacy Policy (Section 4).
- All personnel, including employees, contractors (e.g., in Vietnam and the Philippines for JR Plus platforms), visitors, and vendors accessing Gibble's facilities.

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

2.2 It complements the Security Policy (Section 11), Access Control Policy (Section 7), Employee and Contractor Security Policy (Section 5.5), and Vendor Management Policy (Section 5) to ensure holistic protection of assets and data.

3. Definitions

- 3.1 **Physical Security:** Measures to protect buildings, equipment, and personnel from unauthorised access, theft, damage, or disruption.
- 3.2 **Sensitive Assets:** Physical items containing or providing access to personal information, such as servers, hard-copy files, and storage devices.
- 3.3 **Visitor:** Any individual who is not an employee or contractor, including customers, vendors, or guests.
- 3.4 **Access Controls:** Mechanisms like locks, badges, and biometrics to restrict entry to authorised personnel.

4. Physical Security Principles

- 4.1 **Layered Defence:** Use multiple layers of security controls to protect facilities and assets.
- 4.2 **Access Restriction:** Limit physical access to authorised personnel based on need-to-know and least privilege principles, per the Access Control Policy (Section 4).
- 4.3 **Monitoring and Detection:** Continuously monitor facilities for unauthorised access or suspicious activity.
- 4.4 **Incident Response:** Respond promptly to physical security incidents, integrating with the Information Security Incident Management Policy (Section 8).
- 4.5 **Compliance:** Ensure physical security measures protect personal information in line with data protection laws.

5. Physical Security Controls

5.1 Facility Access:

- **Entry Points:** All office doors and windows are secured with electronic locks and alarms.
- **Biometric Access:** Use fingerprint or facial recognition for entry to sensitive areas (e.g., server rooms, file storage), per the Access Control Policy (Section 7.1).
- **Key Cards/Badges:** Employees and contractors are issued photo ID badges with RFID for access tracking.
- **Visitor Management:** Visitors must sign in at reception, receive temporary badges, and be escorted by authorised personnel. Visitor logs are maintained for 1 year.

5.2 Surveillance and Monitoring:

- **CCTV Systems:** 24/7 video surveillance covers all entry points, common areas, and sensitive zones, with footage retained for 90 days.
- **Alarm Systems:** Intrusion alarms trigger notifications to the Security Officer and local authorities, per the Information Security Incident Management Policy (Section 6).

5.3 Asset Protection:

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

- **Sensitive Assets:** Servers, hard-copy records, and storage devices are stored in locked cabinets or rooms with restricted access.
- **Environmental Controls:** Fire suppression systems, temperature/humidity monitoring, and uninterruptible power supplies (UPS) protect assets from environmental threats, per the Business Continuity and Disaster Recovery Policy (Section 11.2).
- **Inventory Management:** Physical assets are inventoried annually, with serial numbers tracked for accountability.

5.4 Third-Party Facilities:

- Data centres (e.g., AWS, Microsoft) are selected based on compliance with ISO 27001 and physical security certifications, per the Vendor Management Policy (Section 5).
- Vendors must provide access logs and security reports upon request.

6. Procedures

6.1 Access Provisioning:

- Access to facilities is granted based on role, with approval from the Security Officer.
- New employees and contractors receive badges and training during onboarding, per the Employee and Contractor Security Policy (Section 7).
- Access is reviewed quarterly and revoked immediately upon termination, per the Access Control Policy (Section 6.3).

6.2 Visitor Procedures:

- Visitors must pre-register and provide identification.
- Escorts monitor visitors at all times, ensuring no access to sensitive areas.
- Visitors sign non-disclosure agreements (NDAs) if accessing confidential information.

6.3 Incident Reporting:

- Report physical security incidents (e.g., unauthorised entry, theft) to security@gibble.com.au within 1 hour, per the Information Security Incident Management Policy (Section 6).
- Incidents involving data breaches are escalated to the Data Breach Response Team, per the Data Breach Response Plan (Section 5).

6.4 Emergency Response:

- Evacuation procedures are posted and tested annually, per the Business Continuity and Disaster Recovery Policy (Section 11).
- Emergency contacts include local authorities and the Security Officer.

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

7. Monitoring and Auditing

7.1 Monitoring:

- Surveillance and alarm systems are monitored 24/7 by the Facility Manager, with alerts sent to the Security Officer.
- Access logs from badges and biometrics are reviewed daily for anomalies.

7.2 Auditing:

- Quarterly audits verify compliance with physical security controls, including access logs and surveillance footage.
- Audit reports are available to customers upon request at security@gibble.com.au.

8. Roles and Responsibilities

8.1 Security Officer:

- Oversees physical security implementation and compliance.
- Approves access requests and reviews logs.
- Investigates incidents and coordinates responses.

8.2 Facility Manager:

- Manages day-to-day operations, including visitor registration and maintenance of security systems.
- Ensures environmental controls are operational.

8.3 HR Manager:

- Coordinates onboarding and offboarding for access provisioning.
- Ensures confidentiality agreements cover physical security obligations.

8.4 Employees and Contractors:

- Comply with access procedures and report suspicious activity to security@gibble.com.au within 1 hour.
- Escort visitors and secure assets, per the Employee and Contractor Security Policy (Section 5).

8.5 Vendors:

- Comply with physical security requirements when accessing facilities, per the Vendor Management Policy (Section 5).
- Report incidents involving their personnel.

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

9. Training

9.1 Employees and contractors receive annual training on:

- Physical security procedures, including access controls and incident reporting.
- Recognising and responding to physical threats (e.g., tailgating, theft).
- Compliance with this Policy and related policies.

9.2 Visitors receive a briefing on security rules upon entry.

10. Compliance

10.1 This Policy aligns with:

- ISO 27001 A.11 (Physical and Environmental Security).
- GDPR Article 32 (Security of Processing).
- APP 11 (Security of Personal Information).
- NIST 800-53 PE-1 (Physical and Environmental Protection).
- PDPA, CCPA/CPRA, and APPI security requirements.

10.2 AWS and Microsoft data centres provide compliant physical security.

11. Violations

11.1 Violations of this Policy (e.g., unauthorised access, failing to escort visitors) 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.

12. Contact Information

12.1 For physical security inquiries or to report incidents, contact:

- **Security Officer:** security@gibble.com.au
- **Data Protection Officer:** privacy@gibble.com.au

Leftorium Pty Ltd (Trading as Gibble) Physical Security Policy

Last updated: July 2025

- **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.