Encryption 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) Encryption Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Encryption Policy

Last updated: July 2025

1. Purpose

1.1 This Encryption Policy ("Policy") outlines the standards and procedures for encrypting data processed by Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our") through our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures the confidentiality, integrity, and security of personal information, customer data, and other sensitive information, including biometric data, during storage, transmission, and processing.

1.2 The Policy integrates with our Security Policy (Sections 4.1, 4.2, 5.2), Access Control Policy (Section 5), and other policies, leveraging Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to implement robust encryption measures.

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/encryption.

2. Scope

2.1 This Policy applies to:

- All data processed by Gibble's platforms, including personal information (e.g., names, contact details, biometric data), customer data, and analytics data, as described in the Privacy Policy (Section 4).
- Data stored on AWS (e.g., S3, RDS, EC2), Microsoft Entra (e.g., Azure Blob Storage, Entra ID), and third-party systems (e.g., Salesforce, Stripe).
- Data in transit between Gibble's systems, customers, end users, employees, contractors, and vendors.
- Physical media (e.g., USB drives, hard-copy records) containing sensitive data.
- All users, including customers, end users, employees, contractors, and vendors.

2.2 It covers encryption for data at rest, in transit, and during processing, complementing the Security Policy (Section 5), Access Control Policy (Section 5), and Vendor Management Policy (Section 5).

3. Definitions

3.1 **Data at Rest**: Data stored in databases, file systems, or physical media (e.g., AWS S3, hard-copy records).

3.2 **Data in Transit**: Data transmitted over networks, including between Gibble's platforms, customers, and third parties.

3.3 **Data in Processing**: Data actively used by applications or systems during operations.

3.4 **Encryption**: The process of converting data into a secure format to prevent unauthorised access, using cryptographic algorithms.

3.5 **Key Management**: The process of generating, storing, distributing, rotating, and revoking encryption keys.

4. Encryption Principles

4.1 **Confidentiality**: Encryption protects sensitive data from unauthorised access.

4.2 **Integrity**: Encryption ensures data is not altered or corrupted during storage or transmission.

4.3 **Compliance**: Encryption meets or exceeds industry standards and regulatory requirements (e.g., GDPR, ISO 27001).

4.4 **Least Privilege**: Access to encryption keys is restricted to authorised personnel, per the Access Control Policy (Section 5).

4.5 **Continuous Monitoring**: Encryption processes are monitored for integrity and misuse, per the Information Security Incident Management Policy (Section 6).

5. Encryption Standards

5.1 **Data at Rest**:

- **Algorithm**: AES-256 (Advanced Encryption Standard with 256-bit keys).
- **Implementation**:
    - AWS: Server-side encryption with AWS Key Management Service (KMS) for S3, RDS, and EBS.

- Microsoft Entra: Azure Blob Storage and Azure SQL Database use AES-256 encryption.
- On-premises: Encrypted storage devices with AES-256 for physical servers.

- **Sensitive Data**: Biometric data, payroll records, and customer billing information are encrypted by default.

5.2 **Data in Transit**:

- **Protocol**: TLS 1.3 (Transport Layer Security) for all network communications.
- **Implementation**:
  - Web traffic: HTTPS enforced for platform access and website (www.gibble.com.au).
  - APIs: OAuth 2.0 and encrypted API keys via AWS API Gateway.
  - Email: Secure email transmission using TLS 1.3 for communications (e.g., privacy@gibble.com.au).
- **Certificates**: Use of trusted Certificate Authorities (CAs) with annual renewal.

5.3 **Data in Processing**:

- **Encryption**: Homomorphic or partial encryption where feasible to protect data during processing.
- **Implementation**: Secure enclaves (e.g., AWS Nitro Enclaves) for sensitive operations like biometric data processing.
- **Access Controls**: Processing environments restrict access via AWS IAM and Entra ID, per the Access Control Policy (Section 5).

5.4 **Physical Media**:

- Hard-copy records and physical media (e.g., USB drives) are encrypted with AES-256 before storage or transfer.
- Physical media is securely destroyed when no longer needed, per the Data Retention and Deletion Policy (Section 6).

6. Key Management

6.1 **Key Generation**:

- Encryption keys are generated using cryptographically secure random number generators.
- Managed via AWS KMS and Azure Key Vault for automated key creation.

6.2 **Key Storage**:

- Keys are stored in secure hardware security modules (HSMs) within AWS KMS and Azure Key Vault.
- Access to keys is restricted to authorised personnel via role-based access control (RBAC) and multi-factor authentication (MFA), per the Access Control Policy (Section 5).

6.3 **Key Rotation**:

- Keys are rotated annually or immediately if compromise is suspected.
- Automated rotation is configured in AWS KMS and Azure Key Vault, with audit logs maintained.

6.4 **Key Revocation**:

- Compromised or unused keys are revoked immediately via AWS KMS or Azure Key Vault.
- Revocation events are logged and monitored by Adlumin MDR.

6.5 **Key Distribution**:

- Keys are not shared outside secure systems unless encrypted and transmitted via secure channels (e.g., TLS 1.3).
- Third-party vendors receive keys only through secure APIs or DPAs, per the Vendor Management Policy (Section 5).

7. Monitoring and Auditing

7.1 **Monitoring**:

- Adlumin MDR monitors encryption processes for anomalies (e.g., unauthorised key access, decryption attempts).
- AWS CloudTrail and Microsoft Defender for Cloud log encryption-related events (e.g., key usage, API calls).

7.2 **Auditing**:

- Quarterly audits verify encryption compliance with this Policy and regulatory standards.
- Annual ISO 27001 and SOC 2 Type II audits include encryption practices.
- Audit reports are available to customers upon request at security@gibble.com.au.

7.3 **Incident Detection**:

- Encryption-related incidents (e.g., key compromise) are treated as security incidents, managed per the Information Security Incident Management Policy (Section 8).
- Adlumin MDR provides real-time alerts and forensic analysis for encryption incidents.

8. Compliance

8.1 This Policy aligns with:

- ISO 27001 A.10 (Cryptography).
- GDPR Article 32 (Security of Processing).
- APP 11.1 (Security of Personal Information).

- NIST 800-53 SC-13 (Cryptographic Protection).
- FIPS 140-2 for cryptographic modules.
- PDPA, CCPA/CPRA, and APPI security requirements.

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

9. Roles and Responsibilities

9.1 **Security Officer**:

- Oversees encryption implementation and compliance.
- Manages key rotation and revocation processes.
- Investigates encryption-related incidents with Adlumin MDR.

9.2 **IT Manager**:

- Configures encryption settings in AWS KMS, Azure Key Vault, and platform databases.
- Ensures encryption for data at rest, in transit, and during processing.
- Verifies encryption integrity during audits.

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

- Ensures encryption aligns with data protection laws.
- Addresses data subject inquiries related to encryption (privacy@gibble.com.au).

9.4 **Employees and Contractors**:

- Use encrypted systems and report issues to security@gibble.com.au within 1 hour, per the Information Security Incident Management Policy (Section 6).
- Complete annual training on encryption policies.

9.5 **Vendors**:

- Comply with encryption requirements in DPAs, per the Vendor Management Policy (Section 5).
- Use AES-256 and TLS 1.3 for data processing and transmission.

10. Training

10.1 Employees and contractors receive annual training on:

- Encryption standards and best practices.

- Key management procedures.
- Recognising and reporting encryption-related incidents.

10.2 Customers receive guidance on encryption requirements during onboarding, per the Acceptable Use Policy (Section 5).

11. Violations

11.1 Violations of this Policy (e.g., bypassing encryption, unauthorised key access) may result in:

- Immediate suspension of access, per the Access Control Policy (Section 12).
- Disciplinary action for employees or contractors.
- 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.

12. Contact Information

12.1 For encryption-related inquiries or to report issues, contact:

- **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.