Data Breach Response Plan

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) Data Breach Response Plan

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Data Breach Response Plan

Last updated: July 2025

1. Purpose

1.1 This Data Breach Response Plan ("Plan") outlines the procedures Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), follows to detect, assess, contain, notify, and recover from a data breach involving personal information or customer data processed via our SaaS platforms for learning, payroll, student management, and human resources management.

1.2 The Plan ensures compliance with applicable data protection laws, including:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly the Notifiable Data Breaches (NDB) scheme.
- EU General Data Protection Regulation 2016/679 (GDPR), Articles 33 and 34.
- *Privacy Act 2020* (New Zealand), mandatory breach notification requirements.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI).

1.3 The Plan integrates with our Security Policy, leveraging Adlumin Managed Detection and Response (MDR) services, AWS, and Microsoft Entra infrastructure to ensure rapid detection and response.

1.4 For inquiries, contact our Data Protection Officer (DPO) and 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

2. Scope

2.1 This Plan applies to:

- All personal information and customer data processed by Gibble's platforms, including data stored on AWS and Microsoft Entra infrastructure.
- Breaches involving unauthorized access, disclosure, loss, or alteration of data, whether accidental or malicious.
- Internal systems, employee devices, third-party integrations, and data processed by contractors (e.g., in Vietnam and the Philippines for Gibble platforms).

2.2 It covers breaches affecting customers, end users, data subjects, employees, and contractors in Australia, New Zealand, the EU, UK, Singapore, USA, and Japan.

3. Definitions

3.1 Data Breach: An incident where personal information or customer data is accessed, disclosed, lost, or altered without authorization, likely to result in serious harm to individuals or Gibble.

3.2 Eligible Data Breach (Australia): A breach under the NDB scheme where:

- Unauthorized access or disclosure is likely to result in serious harm to individuals.
- Loss of data is likely to lead to unauthorized access or disclosure with serious harm.
- Remediation cannot prevent the likelihood of serious harm.

3.3 Personal Information: Any information relating to an identified or identifiable individual, including names, contact details, payroll data, biometric data, or IP addresses, as defined by applicable laws.

3.4 Serious Harm: Includes physical, psychological, emotional, financial, or reputational harm, as assessed under the NDB scheme, GDPR, or other regulations.

4. Data Breach Response Team

4.1 The Data Breach Response Team (DBRT) is responsible for managing breaches and includes:

- Data Protection Officer (DPO): Oversees compliance and notifications (contact: privacy@gibble.com.au).
- Security Officer: Coordinates technical response and liaises with Adlumin MDR (contact: security@gibble.com.au).
- IT Manager: Manages infrastructure containment and recovery on AWS and Microsoft Entra.
- Legal Counsel: Advises on regulatory obligations and liability.
- Communications Lead: Handles internal and external communications, including customer notifications.
- HR Representative: Addresses breaches involving employee or contractor data.

4.2 The DBRT is activated immediately upon detection of a potential breach and reports to the Chief Executive Officer (CEO).

5. Detection and Reporting

5.1 Detection Mechanisms:

- Adlumin MDR provides 24/7 monitoring, using AI-driven analytics and behavioural analysis to detect threats across AWS, Microsoft Entra, and on-premises systems.
- AWS CloudTrail, Amazon GuardDuty, and Microsoft Defender for Cloud alert on suspicious activities (e.g., unauthorized access, anomalous API calls).
- Employee and contractor reports via security@gibble.com.au for suspected incidents.

- Customer reports through platform support channels or direct contact.

5.2 Internal Reporting:

- All employees and contractors must report suspected breaches to the Security Officer within 1 hour of detection.
- Reports should include:
    - Date and time of detection.
    - Nature of the incident (e.g., unauthorized access, data loss).
    - Affected systems or data (if known).
    - Initial observations on impact.

5.3 Adlumin MDR Role:

- Automatically detects and classifies incidents within minutes.
- Provides initial incident reports to the Security Officer, including threat type, affected systems, and scope.

6. Assessment

6.1 Initial Assessment (within 12 hours):

- The DBRT, with Adlumin MDR support, assesses:
    - Whether a data breach has occurred.
    - The type and sensitivity of data involved (e.g., personal information, biometric data).
    - The likelihood and severity of serious harm to individuals.
    - Whether the breach meets notification thresholds (e.g., NDB scheme, GDPR Article 33).
- Adlumin provides forensic analysis, including log correlation and threat intelligence.

6.2 Criteria for Serious Harm:

- Nature of data (e.g., financial, health, or biometric data increases risk).
- Volume of data affected.
- Potential for identity theft, fraud, or reputational damage.
- Vulnerability of affected individuals (e.g., minors, employees).

6.3 Documentation:

- All findings are recorded in a secure incident log, including:
    - Incident timeline.

- Affected data categories and individuals.
- Preliminary risk assessment.
- Actions taken (e.g., containment measures).

6.4 Escalation:

- If the breach is likely to cause serious harm, the DBRT escalates to a full response within 24 hours.
- If no serious harm is likely, the incident is documented, and preventive measures are implemented.

7. Containment

7.1 Immediate Containment (within 24 hours):

- The Security Officer, with Adlumin MDR and IT Manager, implements containment measures, such as:
  - Isolating affected systems (e.g., disabling compromised AWS EC2 instances or Entra accounts).
  - Revoking unauthorized access credentials via AWS IAM or Entra ID.
  - Blocking malicious IP addresses using AWS WAF or Microsoft Defender.
  - Patching vulnerabilities identified by Adlumin or AWS GuardDuty.
- Adlumin automates containment where possible (e.g., quarantining malware).

7.2 Short-Term Containment:

- Deploy temporary firewalls or access restrictions.
- Redirect platform traffic to unaffected servers.
- Preserve evidence (e.g., logs, snapshots) for forensic analysis.

7.3 Long-Term Containment:

- Implement permanent fixes (e.g., software patches, configuration changes).
- Update access controls and encryption protocols if compromised.

8. Notification

8.1 Regulatory Notification:

- Australia (NDB Scheme): If an eligible data breach is confirmed, the DPO notifies the Office of the Australian Information Commissioner (OAIC) within 30 days of suspicion, or sooner if practicable, via the OAIC's online form.
- EU/UK (GDPR): The DPO notifies the relevant supervisory authority (e.g., ICO in the UK) within 72 hours of becoming aware of the breach, unless serious harm is unlikely.

- New Zealand: The DPO notifies the Office of the Privacy Commissioner within 72 hours if serious harm is likely.
- Singapore (PDPA): Notification to the Personal Data Protection Commission within 72 hours if significant harm or scale is confirmed.
- USA (CCPA/CPRA): Notification to the California Attorney General if required under state law.
- Japan (APPI): Notification to the Personal Information Protection Commission as per regulatory guidelines.

8.2 Customer Notification:

- Customers are notified within 72 hours if their data or data subjects are affected, unless serious harm is unlikely.
- Notifications include:
    - Description of the breach and affected data.
    - Potential risks to data subjects.
    - Mitigation steps taken (e.g., password resets).
    - Contact details for further inquiries (privacy@gibble.com.au).
- Customers are responsible for notifying their data subjects, as per our Privacy Policy.

8.3 Data Subject Notification:

- If customers cannot notify data subjects, Gibble may do so directly (e.g., via email or platform alerts) with customer approval, including:
    - Nature of the breach.
    - Recommended actions (e.g., monitoring financial accounts).
    - Support resources (e.g., identity theft protection services).

8.4 Public Communication:

- The Communications Lead, with Legal Counsel approval, issues public statements if required, posted at www.gibble.com.au/security.

9. Recovery

9.1 System Restoration:

- The IT Manager restores affected systems using encrypted backups from AWS S3 or Azure Blob Storage.
- Systems are tested for integrity before resuming operations.
- Adlumin MDR verifies no residual threats remain.

9.2 Preventive Measures:

- Conduct root cause analysis with Adlumin's forensic reports.

- Implement corrective actions, such as:
    - Updating security configurations (e.g., AWS IAM policies, Entra conditional access).
    - Patching software vulnerabilities.
    - Enhancing employee training on phishing or social engineering.

9.3 Monitoring:

- Adlumin MDR increases monitoring for 90 days post-breach to detect related threats.
- AWS GuardDuty and Microsoft Defender provide enhanced analytics.

10. 10. Documentation and Review

10.1 Incident Log:

- The DPO maintains a secure incident log, including:
    - Breach details and timeline.
    - Assessment findings and risk level.
    - Containment, notification, and recovery actions.
    - Lessons learned and preventive measures.

10.2 Post-Incident Review:

- Within 30 days, the DBRT conducts a review to:
    - Evaluate response effectiveness.
    - Identify gaps in security controls.
    - Update the Plan, Security Policy, or training programs.

10.3 Audit Trail:

- Adlumin MDR provides automated compliance reports for regulators and auditors.
- Logs are retained for 7 years, per Australian tax and privacy requirements.

11. Employee and Contractor Responsibilities

11.1 All employees and contractors must:

- Report suspected breaches immediately to security@gibble.com.au.
- Cooperate with the DBRT during investigations.
- Complete annual training on breach detection and response.

11.2 Failure to comply may result in disciplinary action, per employment or contractor agreements.

12. Third-Party Responsibilities

12.1 Third-party providers (e.g., AWS, Microsoft, Adlumin, Stripe) are contractually obligated to:

- Notify Gibble of breaches affecting our data within 24 hours.
- Support forensic investigations and remediation.
- Comply with GDPR, APPs, and other applicable laws via Data Protection Agreements (DPAs).

12.2 Contractors in Vietnam and the Philippines (e.g., for Gibble platforms) follow strict security protocols and report breaches to Gibble's Security Officer.

13. Compliance and Testing

13.1 Compliance:

- The Plan aligns with ISO 27001, NIST Cybersecurity Framework, and regional regulations.
- AWS and Microsoft Entra compliance dashboards track adherence to GDPR, CCPA, PDPA, and APPI.
- Adlumin MDR provides audit-ready reports for regulatory inspections.

13.2 Testing:

- Annual tabletop exercises simulate breaches to test DBRT readiness.
- Quarterly reviews ensure alignment with evolving threats and regulations.
- Penetration testing validates containment and recovery processes.

14. Contact Information

14.1 For breach-related inquiries or reports, contact:

- Data Protection Officer: privacy@gibble.com.au
- Security Officer: security@gibble.com.au
- Phone: +61 3 97442887

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.