Information Security Incident 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

Leftorium Pty Ltd (Trading as Gibble) Information Security Incident Management Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Information Security Incident Management Policy

Last updated: July 2025

1. Purpose

1.1 This Information Security Incident Management Policy ("Policy") outlines the procedures for identifying, assessing, responding to, and recovering from security incidents affecting Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), and our SaaS platforms for learning, payroll, student management, and human resources management. The Policy ensures rapid detection, containment, and resolution of incidents to protect the confidentiality, integrity, and availability of systems and data.

1.2 The Policy complements the Data Breach Response Plan (Section 5) and Security Policy (Section 7), leveraging Adlumin Managed Detection and Response (MDR) services, Amazon Web Services (AWS), and Microsoft Entra infrastructure to manage incidents effectively.

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 33.
- *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/incident-management.

2. Scope

2.1 This Policy applies to:

- All security incidents affecting 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).
- Incidents involving personal information, customer data, analytics data, and system operations, as described in the Privacy Policy (Section 4).
- All users, including customers, end users, employees, contractors, and third-party vendors.
- Physical and digital environments, including Gibble's offices and data centres.

2.2 It covers incidents such as unauthorised access, malware infections, system outages, denial-of-service (DoS) attacks, and data breaches, complementing the Data Breach Response Plan for breaches involving personal information.

3. Definitions

3.1 **Security Incident**: Any event that compromises or threatens to compromise the confidentiality, integrity, or availability of Gibble's systems, data, or operations.

3.2 **Data Breach**: A security incident involving unauthorised access, disclosure, loss, or alteration of personal information, as defined in the Data Breach Response Plan (Section 3).

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

3.4 **Incident Severity**: Classified as Low, Medium, High, or Critical based on impact and urgency.

4. Incident Management Principles

4.1 **Proactive Detection**: Leverage Adlumin MDR, AWS CloudTrail, and Microsoft Defender for Cloud for real-time incident detection.

4.2 **Rapid Response**: Contain and mitigate incidents promptly to minimise damage.

4.3 **Accountability**: Document all incidents, actions, and outcomes for traceability and compliance.

4.4 **Continuous Improvement**: Analyse incidents to enhance security controls and prevent recurrence.

4.5 **Compliance**: Align with ISO 27001, GDPR, and other regulations for incident handling and reporting.

5. Incident Management Team

5.1 The Incident Management Team (IMT), aligned with the Data Breach Response Team (DBRT), includes:

- **Security Officer**: Leads incident response and coordinates with Adlumin MDR.
- **Data Protection Officer (DPO)**: Ensures compliance with data protection laws (privacy@gibble.com.au).
- **IT Manager**: Manages technical containment and recovery on AWS and Entra infrastructure.

- **Legal Counsel**: Advises on regulatory obligations and liability.
- **Communications Lead**: Handles internal and external communications.
- **HR Representative**: Addresses incidents involving employee or contractor data.

5.2 The IMT reports to the Chief Executive Officer (CEO) and is activated immediately upon incident detection.

6. Incident Detection and Reporting

6.1 **Detection Mechanisms**:

- Adlumin MDR provides 24/7 monitoring with AI-driven analytics and behavioural analysis to detect threats (e.g., malware, unauthorised access).
- AWS CloudTrail and Amazon GuardDuty monitor infrastructure for suspicious activities (e.g., anomalous API calls).
- Microsoft Defender for Cloud detects threats in Entra ID and Azure environments.
- Employees, contractors, customers, and vendors report incidents via security@gibble.com.au or www.gibble.com.au/report.

6.2 **Internal Reporting**:

- All users must report suspected incidents within 1 hour, including:
    - Date and time of detection.
    - Nature of the incident (e.g., system outage, malware).
    - Affected systems or data (if known).
- Reports are submitted to the Security Officer for triage.

6.3 **Adlumin MDR Role**:

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

7. Incident Assessment

7.1 **Initial Assessment** (within 12 hours):

- The IMT, with Adlumin MDR support, assesses:
    - Incident type (e.g., malware, DoS, unauthorised access).
    - Severity (Low, Medium, High, Critical) based on:

        - Impact on system availability, data integrity, or confidentiality.
        - Potential harm to customers, end users, or Gibble's operations.
    - Whether the incident qualifies as a data breach (Data Breach Response Plan, Section 6).
- Adlumin MDR provides forensic analysis, including log correlation and threat intelligence.

7.2 **Severity Classification**:

- **Low**: Minimal impact (e.g., failed login attempts with no data compromise).
- **Medium**: Limited impact (e.g., temporary system outage, no data loss).
- **High**: Significant impact (e.g., malware affecting multiple systems, potential data exposure).
- **Critical**: Severe impact (e.g., data breach, widespread system compromise).

7.3 **Documentation**:

- All incidents are recorded in a secure incident log, including:
    - Incident description and timeline.
    - Affected systems, data, or users.
    - Initial severity assessment and actions taken.

8. Incident Containment

8.1 **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 AWS EC2 instances, Entra accounts).
    - Blocking malicious IP addresses via AWS Web Application Firewall (WAF) or Microsoft Defender.
    - Revoking compromised credentials via AWS IAM or Entra ID (Access Control Policy, Section 6).
    - Deploying patches for identified vulnerabilities.
- Adlumin MDR automates containment (e.g., quarantining malware).

8.2 **Short-Term Containment**:

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

8.3 **Long-Term Containment**:

- Implement permanent fixes (e.g., software updates, configuration changes).
- Update access controls and encryption protocols if compromised, per the Access Control Policy (Section 5).

9. Incident Eradication and Recovery

9.1 **Eradication**:

- Remove malicious elements (e.g., malware, backdoors) using Adlumin MDR and AWS/Microsoft tools.
- Patch vulnerabilities identified during the incident.
- Verify eradication through Adlumin MDR scans and penetration testing.

9.2 **Recovery**:

- Restore systems from encrypted backups in AWS S3 or Azure Blob Storage, per the Security Policy (Section 5.5).
- Test restored systems for integrity before resuming operations.
- Adlumin MDR confirms no residual threats remain.

9.3 **Customer Impact**:

- Notify customers of service disruptions or data impacts, per the Data Breach Response Plan (Section 8).
- Provide recovery timelines and support via support@gibble.com.au.

10. Notification

10.1 **Regulatory Notification**:

- For data breaches, follow the Data Breach Response Plan (Section 8), including:
    - Australia: Notify the Office of the Australian Information Commissioner (OAIC) within 30 days for eligible data breaches.
    - EU/UK: Notify supervisory authorities (e.g., ICO) within 72 hours per GDPR Article 33.
    - New Zealand: Notify the Privacy Commissioner within 72 hours for serious harm.
    - Singapore, USA, Japan: Notify relevant authorities per PDPA, CCPA/CPRA, or APPI requirements.

10.2 **Customer and Data Subject Notification**:

- Customers are notified within 72 hours of high or critical incidents affecting their data, with details on impact and mitigation.

- Data subjects are notified via customers or directly by Gibble if required, per the Privacy Policy (Section 14).

10.3 **Public Communication**:

- The Communications Lead issues statements for critical incidents, posted at www.gibble.com.au/security, with Legal Counsel approval.

11. Post-Incident Review

11.1 **Analysis** (within 30 days):

- Conduct root cause analysis with Adlumin MDR forensic reports.
- Identify gaps in security controls or processes.
- Document lessons learned and preventive measures.

11.2 **Updates**:

- Update security controls, policies (e.g., Access Control Policy, Vendor Management Policy), or training based on findings.
- Implement corrective actions (e.g., enhanced monitoring, patch management).

11.3 **Reporting**:

- A post-incident report is prepared for the CEO and customers (if applicable), detailing:
    - Incident summary and impact.
    - Response and recovery actions.
    - Preventive measures implemented.

12. Roles and Responsibilities

12.1 **Security Officer**:

- Leads incident response and coordinates with Adlumin MDR.
- Ensures documentation and regulatory compliance.

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

- Handles regulatory and customer notifications for data breaches.
- Ensures compliance with data protection laws.

12.3 **IT Manager**:

- Executes technical containment and recovery on AWS and Entra infrastructure.
- Verifies system integrity post-recovery.

12.4 **Employees and Contractors**:

- Report incidents within 1 hour to security@gibble.com.au, per the Acceptable Use Policy (Section 5).
- Cooperate with the IMT during investigations.

12.5 **Vendors**:

- Report incidents within 24 hours, per the Vendor Management Policy (Section 7).
- Provide forensic data and support remediation.

13. Compliance and Auditing

13.1 **Compliance**:

- Aligns with ISO 27001 A.16 (Information Security Incident Management).
- GDPR Article 33, APP 11, NIST 800-61, PDPA, CCPA/CPRA, APPI.

13.2 **Auditing**:

- Quarterly incident management audits verify process effectiveness.
- Annual third-party audits for ISO 27001 and SOC 2 include incident management reviews.
- Adlumin MDR provides audit-ready logs for compliance reporting.

14. Training

14.1 All employees and contractors receive annual training on:

- Incident detection and reporting procedures.
- Recognising threats (e.g., phishing, malware).
- Compliance with this Policy and the Data Breach Response Plan.

14.2 Customers receive guidance on incident reporting during onboarding, per the Acceptable Use Policy (Section 5).

15. Contact Information

15.1 For incident reports or inquiries, contact:

- **Security Officer**: security@gibble.com.au

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

15.2 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.