Lumo

Security and Safety

Secure Architecture and Operational Framework for Data Protection and AI/LINE Integrations

Little Help Agency LLC

Date Issued: April 3, 2026
Last Updated: July 18, 2026

Table of Contents

1. Introduction

1.1 Purpose of This Document

Lumo is an an AI agent for LINE marketing.
This document provides a comprehensive overview of Lumo’s security practices so that customers can use the service with confidence.

- **For Your Peace of Mind**
  This document explains how Lumo meets enterprise-grade security standards.

- **As Supporting Documentation for Security Assessments**
  It may be used as supporting evidence for internal security reviews and third-party assessments.

1.2 Covered Services and Scope

This document covers the following services and systems.

- Lumo Admin Console (Web Application)
- Lumo API (Administrative API / Public API)
- AI Agent Features (Marketing Agent / Customer Agent)
- LINE Integration Features (Webhook Reception / Message Delivery / LINE Login)
- CRM Integration Features (HubSpot / Shopify / Klaviyo)
- Payment Integration Features (Stripe / Paid)
- Related Cloud Infrastructure

1.3 Frameworks Covered by This Document

This document is structured to cover the key requirements of the following major security frameworks and guidelines.

Framework	Issued By	Scope
Cloud Service Level Checklist	Ministry of Economy, Trade and Industry (METI)	Seven categories: availability, reliability, performance, scalability, support, data management, and security
ASP/SaaS Information Disclosure Guidelines	Ministry of Internal Affairs and Communications (MIC)	Key areas including business operations, personnel, compliance, service characteristics, and networks
How to Build a Secure Website	IPA (Information-technology Promotion Agency, Japan)	Mitigation of web application vulnerabilities such as SQL injection, XSS, and CSRF
OWASP Top 10 for LLM Applications 2025	OWASP	AI-specific risks including prompt injection, data leakage, and agent control

For a detailed mapping between each section and the applicable compliance frameworks, please refer to Appendix A.

1.4 Terminology and Notation

Term	Description
GCP	Google Cloud Platform, the cloud infrastructure platform used by Lumo
Cloudflare	An edge security platform providing CDN, DDoS protection, TLS termination, and related services
VPC	Virtual Private Cloud, a logically isolated private network
TLS	Transport Layer Security, a protocol for encrypting communications
AES	Advanced Encryption Standard, a data encryption standard
WAF	Web Application Firewall
RBAC	Role-Based Access Control
LLM	Large Language Model
RAG	Retrieval-Augmented Generation

1.5 Revision History

Version	Date	Changes
1.0	April 3, 2026	Initial release
1.1	July 16, 2026	Clarified the processing regions used for AI operations
2.0	July 17, 2026	Reflected implementation enhancements and comprehensively improved the accuracy of the document
2.1	July 18, 2026	Added information on support access restrictions and logging, and improved the accuracy of the document

2. Service Overview and Certifications

2.1 Overview of Lumo

Lumo is AI agent for LINE marketing that learns more about customers through continued use and helps identify optimized marketing initiatives.
It is developed by an engineering team with extensive expertise in LINE and HubSpot, drawing on years of operational experience gained through its predecessor product, LITTLE HELP CONNECT.

Key Features:

- **Message Delivery:** AI-generated campaign messages, segmented messaging, scenario-based messaging, and A/B testing
- **Analytics:** AI-powered customer profile analysis and recommendations, campaign performance analysis, and improvement recommendations
- **Automation:** AI-assisted automation setup and workflow management
- **Chat:** AI-assisted inquiry handling and automated chat response generation
- **CRM Integrations:** HubSpot, Shopify, and Klaviyo

2.2 Company Information

Item	Details
Company Name	Little Help Agency LLC
English Name	Little Help Agency LLC
Address	xLINK, 3F Shin-Otemachi Building, 2-2-1 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
Established	January 15, 2019
Capital	JPY 5 million
Representative	Shinobu Kawano（JI野忍）
Business Details	Development and sale of LINE marketing tools and provision of related services

2.3 Certifications and Accreditations

Lumo and its operating company have obtained the following certifications and accreditations.

PrivacyMark (P-Mark)

Our handling of personal information is certified by an independent third party. We have obtained PrivacyMark certification from the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) and appropriately maintain and operate a Personal Information Protection Management System (PMS) based on JIS Q 15001.

- Certification No.: 25000199 (02)
- Certifying Organization: Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- Applicable Standard: JIS Q 15001 (Personal Information Protection Management Systems — Requirements)

2.3 Certifications and Accreditations

LY Corporation Certified Technology Partner

Our handling of personal information is certified by an independent third party. We have obtained PrivacyMark certification from the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) and appropriately maintain and operate a Personal Information Protection Management System (PMS) based on JIS Q 15001.

Klaviyo Certified Technology Partner

We are certified as a technology partner of Klaviyo and provide integrations that comply with Klaviyo’s security, privacy, and technical requirements.

2.3 Certifications and Accreditations

HubSpot Certified Technology Partner

We are certified as a technology partner of HubSpot, Inc. and provide applications that comply with HubSpot’s security and privacy standards.

ISO 27001 / SOC 2 Type II

We have not yet obtained ISO 27001 (ISMS) or SOC 2 Type II certification. We will consider pursuing these certifications as the business grows. At present, we maintain enterprise-grade security through PrivacyMark certification, regular external vulnerability assessments, and the security measures described in this document.

2.4 External Security Assessments

Regular Vulnerability Assessments by External Security Specialists

Lumo regularly undergoes vulnerability assessments conducted by external security specialists. We regard these assessments as an important investment in objectively validating product security and protecting customer data.

- **Frequency:** At least once a year, with additional assessments conducted as needed when major features are added
- **Assessment Scope:** Web application, API, and infrastructure
- **Assessment Details:** Vulnerability scanning, including the OWASP Top 10, and penetration testing
- **Response Policy:** Identified vulnerabilities are prioritized based on severity, and remediation is verified through reassessment
- **Sharing Assessment Results:** A summary of the assessment results can be shared for customer security reviews after an NDA has been executed. Please contact us for details
- Most recently, in April 2026, we completed remediation of all 12 issues identified in a third-party assessment conducted by an external security specialist. We maintain a framework that enables prompt remediation and reassessment of all identified issues.

3. Shared Responsibility Model

Security in cloud services is based on a shared responsibility model between the service provider and the customer. This section clarifies the scope of responsibility for each party.

3.1 Lumo’s Responsibilities

Lumo is responsible for security in the following areas.

- **Application Security:** Secure code development, vulnerability mitigation, input validation, and implementation of authentication and authorization
- **Data Protection:** Encryption, backups, tenant isolation, and operation of data retention and deletion policies
- Infrastructure Configuration Management: Secure configuration of cloud resources, network isolation, and access control
- **Operational Security:** Monitoring, log management, incident response, and vulnerability management
- **AI Safety:** Appropriate use of AI models, data handling, and output quality management
- **Compliance:** Compliance with the Act on the Protection of Personal Information and PrivacyMark requirements

3.2 Customer Responsibilities

Customers are responsible for managing the following areas.

- **Account Management:** Proper management of login credentials and activation of two-factor authentication
- **Access Permission Management:** Inviting and removing workspace members and assigning appropriate roles
- **API Key Management:** Secure storage of API keys and deletion of unnecessary keys
- **Content Management:** Verification of the legality of distributed content and confirmation of copyright and trademark compliance
- **Handling of Personal Data:** When handling the personal data of end users, including LINE users, through Lumo, customers are responsible for obtaining appropriate consent and maintaining an appropriate privacy policy
- **Compliance with Terms of Use:** Compliance with our Terms of Service and the terms of use of each integrated service

3.3 Cloud Infrastructure Provider Responsibilities

Google Cloud Platform (GCP)

GCP is responsible for the following areas.

- **Physical Security:** Physical protection of data centers, access control, and monitoring
- **Hardware:** Security of servers, storage, and network equipment
- **Infrastructure Software:** Management of hypervisors, host operating systems, and network infrastructure
- **Certifications:** Certified under standards including SOC 1/2/3, ISO 27001/27017/27018, and PCI DSS

Cloudflare

Cloudflare primarily provides the following functions for Lumo’s public-facing traffic.

- **Edge Security:** DDoS protection and TLS termination
- **Network:** Operation of a global CDN network and maintenance of availability
- **Certifications:** Certified under standards including SOC 2 Type II, ISO 27001, and PCI DSS

4. Organizational and Personnel Security

We safeguard customer data through a highly reliable framework backed by years of operational experience. Our handling of personal information is certified by an independent third party through the PrivacyMark program.

4.1 Information Security Policy

We have established a basic information security policy that is followed throughout the organization.

- **Status:** Established and operated as a personal information protection policy based on PrivacyMark certification
- **Review Frequency:** Once every two years, in conjunction with the PrivacyMark renewal review
- **Scope:** All relevant parties, including all employees and contractors
- **Core Principles:** Ensuring confidentiality, integrity, and availability; legal compliance; and continuous improvement

4.2 Information Security Management Structure

- **Chief Officer:** The representative member bears ultimate responsibility for information security
- **Personal Information Protection Manager:** A Personal Information Protection Manager is appointed in accordance with PrivacyMark requirements
- **Review:** We conduct regular internal audits and make continuous improvements

4.3 Employee Security Education and Training

- **Frequency:** At least once a year, including onboarding and regular training
- **Users:** All personnel, including full-time employees, contract employees, and contractors
- **Details:**
  - Communication of the information security policy and confirmation of understanding
  - Handling of personal information in accordance with PrivacyMark requirements
  - Incident reporting procedures and escalation paths
  - Measures against phishing and social engineering
- **Record Management:** Training records are retained and managed

4.4 Non-Disclosure Agreements (NDAs)

- We enter into employment agreements containing confidentiality provisions with all employees
- We also enter into NDAs with contractors and restrict how information may be handled
- Confidentiality obligations remain in effect for a specified period after employment ends

4.5 Contractor Management

- We assess the security framework of contractors during the selection process
- We enter into agreements with contractors that include security requirements
- When subcontracting the handling of personal data to a third party, we provide prior notice to the customer and obtain the customer’s written consent before proceeding (Article 6 of the Data Processing Agreement)
- We regularly review the management status of contractors

4.6 Legal and Regulatory Compliance

We comply with the following laws and standards.

- **Act on the Protection of Personal Information** (APPI)
- **JIS Q 15001** (Personal Information Protection Management Systems — Requirements)
- **Telecommunications Business Act** (Protection of the Secrecy of Communications)
- **Act on Prohibition of Unauthorized Computer Access**

By obtaining and maintaining PrivacyMark certification (No. 25000199 (02)), the appropriate operation of our Personal Information Protection Management System is continuously assessed by an independent third party.

Cross-Border Data Transfers

When Lumo integrates with certain external services, some customer data may be processed on servers outside Japan. These services hold certifications such as SOC 2 Type II and ISO 27001 and implement appropriate data protection measures. Data sent to external services is limited to the minimum necessary to provide each service's functionality. For details, Section 12, External Service Integration Security, and Appendix B

5. Infrastructure Security

Lumo’s infrastructure is built primarily on Google Cloud Platform and Cloudflare. We protect customer data through multiple layers of security.

5.1 Cloud Infrastructure (Google Cloud Platform)

Lumo is securely operated on Google Cloud Platform.

- **Region Used:** Tokyo, Japan
- **Data Location:** Japan
- The GCP Tokyo region is operated in facilities certified under standards including ISO 27001 and SOC 2 Type II

Key GCP services used include a serverless container runtime, fully managed databases, messaging infrastructure, secret management, AI infrastructure, and monitoring and logging platforms.

5.2 Network Security

- **Virtual Private Cloud (VPC):** We maintain a dedicated VPC and separate the application and database layers at the network level
- **Private Database Configuration:** Databases use private IP addresses only and are designed to prevent direct access from the internet
- **Access Restrictions:** Administrative access to databases is restricted to a dedicated access path authenticated through IAP (Identity-Aware Proxy). Direct connections from the internet are not permitted.
- **Outbound Traffic Control:** Outbound communications pass through a NAT gateway to manage IP addresses and control traffic

5.3 Edge Security (Cloudflare)

All public-facing services are routed through Cloudflare and are protected and controlled as follows.

Feature	Description
DDoS Protection	Automatically detects and mitigates large-scale distributed denial-of-service attacks
TLS Termination	TLS termination at the edge ensures HTTPS communications
Centralized Public Traffic Routing	Routes traffic to public-facing services through Cloudflare, enabling centralized control and monitoring at the edge

5.4 Encryption in Transit

All communications are encrypted and protected using SSL/TLS.

- Communications with clients are encrypted using TLS 1.2 or later, with TLS 1.3 used at the edge
- The minimum TLS version at the edge (TLS 1.2 or later) and HTTPS enforcement settings are managed using Terraform (Infrastructure as Code), enabling configuration changes to be tracked.
- All internal communications between services are also encrypted
- HTTP access is automatically redirected to HTTPS
- Unencrypted HTTP communications are not permitted

5.5 Container Runtime Environment

- Each service runs in a sandboxed container environment
- Access to internal services is restricted through IAM authentication, preventing direct external access
- Automatic scaling based on load helps maintain availability
- Each deployment runs as a new container image without modifying the existing environment

6. Data Protection

Data is managed by contract and is not used to retrain external AI models. Customer data is appropriately classified and protected according to its classification.

6.1 Data Classification

Lumo classifies the data it handles into the following four levels and applies appropriate protective measures to each.

Category	Examples	Protection Measures
Critical	Passwords, authentication tokens, and encryption keys	Hashing or application-level encryption, with all access logged
High	Email addresses, phone numbers, names, and LINE information	Application-level encryption and access control through workspace authentication
Medium	Campaign data, message delivery history, and segment settings	Workspace access controls and logging of changes and deletions
Low	Public configuration information and UI theme settings	Standard access controls

6.2 Encryption at Rest

Data is continuously backed up automatically, with multiple layers of encryption applied at rest.

Infrastructure-Level Encryption

- **Database:** AES-256 encryption at rest is automatically applied by GCP
- **File Storage:** AES-256 encryption at rest is automatically applied by Cloudflare

Application-Level Encryption

In addition to infrastructure-level encryption, sensitive data is protected with additional application-level encryption.

- **User Passwords:** Hashed using an industry-standard hashing algorithm and never stored in plaintext
- **Authentication Tokens and Private Keys:** AES-256 encryption
- **Authentication Credentials for External Service Integrations:** AES-256 encryption
- **API Keys:** Stored using a one-way hash and never retained in plaintext

6.3 Encryption in Transit

- All external communications are encrypted using TLS 1.2 or later
- Communications between internal services are also encrypted
- Unencrypted HTTP communications are not permitted

6.4 Data Location

Data Type	Storage Location
Database	GCP Tokyo Region (Japan)
File Storage	Cloudflare R2 Asia-Pacific Region
Backups	GCP Tokyo Region (Japan)

Customer primary data (databases) and backups are stored in Japan.

Files such as images and other assets are stored in the Asia-Pacific region.

6.5 Backup and Recovery

Automated Backups

- **Backup Frequency:** In addition to weekly full backups, continuous backups using point-in-time recovery (PITR) are performed automatically.
- **Point-in-Time Recovery (PITR):** Data can be restored to any point in time
- **Multiple Backup Generations:** Multiple backup generations are retained for recovery in the event of a failure
- **Deletion Protection:** Database deletion protection is enabled in production to prevent accidental deletion

Recovery Objectives

Metric	Target
RTO (Recovery Time Objective)	Less than 1 hour
RPO (Recovery Point Objective)	Less than 5 minutes

6.6 Data Retention and Deletion Policy

- Appropriate retention periods are established for each data type, and data is deleted once the applicable retention period has expired.
- Audit logs are retained in the production environment for one year. This retention period is enforced through the Cloud Logging retention settings.

6.6 Data Retention and Deletion Policy

Data Deletion Upon Contract Termination

1. **Immediate Logical Deletion:** Upon receiving a deletion request, the applicable workspace is immediately placed in a logically deleted state. All access is blocked, and integrations with external services are disabled.
2. **30-Business-Day Retention Period:** A 30-business-day retention period is provided to allow for accidental deletion or withdrawal of the request. Data can be restored during this period.
3. **Physical Deletion:** After the retention period has expired, the data is physically deleted.
4. **Issuance of a Deletion Certificate:** Once physical deletion is complete, a deletion certificate is issued. The certificate includes the identifier of the applicable workspace, the date and time of deletion, a summary of the deleted data, and our signature (Article 9 of the Data Processing Agreement).
5. **Deletion from Backups:** Following physical deletion, any remaining data in backups is permanently deleted once the applicable backup retention period has expired, which may take up to 14 weeks.
6. If you wish to export your data before contract termination, please contact us.

6.7 Multi-Tenant Data Isolation

Data is strictly isolated by contract (workspace).

- **Database-Level Isolation Controls:** As a general rule, all tenant data must be associated with a workspace, except for explicitly defined exceptions such as operational telemetry. This structure prevents data from being accessed across tenants.
- **Automated Enforcement in CI:** Continuous integration (CI) automatically verifies that all SQL operations comply with workspace boundaries. Together with schema contract tests, these checks are required before code can be merged. Changes that could compromise tenant isolation are automatically detected and rejected before release.
- **Automated Testing:** Compliance with tenant isolation policies is continuously verified through automated testing.

7. Authentication and Access Control

Lumo combines multiple authentication methods and access controls to protect customer accounts and data.

7.1 Authentication Methods

Authentication Method	Users	Description
Email / Password	Admin Console Users	Passwords are stored using an industry-standard hashing algorithm
Google OAuth	Admin Console Users	Single sign-on using a Google account
Two-Factor Authentication (2FA)	Admin Console Users	Additional authentication using a one-time password
API Keys	API Users	Hashed storage and secure verification
LINE Login	End Users	Authentication using a LINE account

7.2 Two-Factor Authentication (2FA)

Admin console users can enable two-factor authentication to strengthen account security.

- **Method:** Time-based One-Time Password (TOTP), compliant with RFC 6238
- **Supported Apps:** TOTP-compatible apps such as Google Authenticator and Microsoft Authenticator
- **Secret Keys:** Generated using cryptographically secure random values and stored in encrypted form

7.3 Password Policy

- **Complexity Requirements:** Passwords must meet a minimum length and include both letters and numbers
- **Storage Method:** Hashed using an industry-standard hashing algorithm and never stored in plaintext
- **Authentication Protection:** Two-factor authentication (TOTP) is supported. Login responses do not disclose detailed failure reasons, reducing the risk of credential guessing and account enumeration

If a customer’s internal policy requires greater password complexity, users are encouraged to set stronger passwords. We are considering offering administrator-configurable password policies in the future.

7.4 Session Management

- **Token-Based Authentication:** Industry-standard token formats are used
- **Validity Periods:** Appropriate validity periods are set for access and refresh tokens
- **Cookie Protection:** The HttpOnly (not accessible to JavaScript), Secure (HTTPS only), and SameSite=Lax attributes are applied to prevent cookies from being sent unintentionally in cross-site contexts.
- **Multi-Layered CSRF Protection:** In addition to the SameSite attribute, authentication uses a stateless approach based on bearer tokens. This multi-layered architecture reduces the risk of cross-site request forgery (CSRF).
- **Immediate Revocation:** In addition to token signature verification, server-side token management enables immediate revocation

7.5 Role-Based Access Control (RBAC)

The following roles and permissions can be assigned to users within a workspace.

Role	Permissions
Administrator	Has access to all workspace features. Administrators can also perform administrative actions, including inviting and removing members, configuring roles and permissions, managing billing and contracts, and deleting the workspace.
Member	Can use only the features individually authorized by an administrator.

Access permissions can be individually granted or restricted for members on a feature-by-feature basis.

The main features covered include chat flows, templates, tags, broadcasts, LINE accounts, databases, AI documents, reports, workflows, chat, and analytics. For Chat (Inbox), access can also be limited to specific LINE accounts assigned to the member. Administrative actions—including member management, billing management, and workspace deletion—are restricted to the Administrator role and cannot be performed by members.

For every API request, we verify that the requesting user is a member of the applicable workspace.

7.6 API Key Authentication

Access to the Lumo Public API is authenticated using API keys.

- **Generation:** Keys are generated using cryptographically secure random values
- **Storage:** Keys are stored using a one-way hash; plaintext API keys are never stored
- **Secure Verification:** A verification method designed to prevent timing attacks is used

7.7 Secret Management

- **Management Platform:** All secrets are centrally managed using GCP Secret Manager
- **Principle of Least Privilege:** Each service is granted only the minimum permissions required
- **Keyless Authentication:** The deployment process does not retain long-lived authentication keys
- **Environment Isolation:** Separate projects and secrets are used for development and production
- **Rotation Policy:** Secrets are rotated annually or immediately in the event of an incident

7.8 Access Restrictions for Our Personnel (Support Access)

Our personnel may access a customer's workspace to respond to customer inquiries and provide other support.

The following restrictions and logging requirements apply to such access:

- **Restricted by Allowlist:** Support access is limited to accounts explicitly designated in an allowlist.
- **Read-Only Access:** Support access is restricted to read-only. Our personnel cannot create, modify, or delete customer data. Write operations are technically blocked.
- **Logging of All Access:** All actions performed through support access are recorded in security logs, including the individual who performed the action, the applicable workspace, the date and time, and the details of the action. These records can be traced retrospectively.

8. Application Security

Security is integrated into every stage of Lumo’s development process. In addition, regular vulnerability assessments by external specialists provide objective validation of the product’s security.

8.1 Secure Development Lifecycle

We have established a development framework that integrates security into the development process.

Process	Details
Code Review	All code changes undergo a security review by another developer before release
Static Analysis	Automated code analysis detects quality and security issues
Dependency Management	Vulnerabilities in third-party libraries are detected automatically to continuously maintain security
Automated Testing	Automated tests and build verification are performed before release
Environment Isolation	Development and production environments are fully separated to prevent unnecessary access to production data

8.2 Vulnerability Assessments

Regular vulnerability assessments are conducted **by external security specialists to continuously verify product security.**

- **Frequency:** At least once a year, with additional assessments conducted as needed when major features are added
- **Most Recent Assessment:** Completed in fiscal year 2026
- **Assessment Types:** Web application, API, and platform assessments
- **Response Process for Identified Vulnerabilities:**
  - Severity classification (Critical / High / Medium / Low)
  - Remediation deadlines based on severity
  - Reassessment after remediation
  - Progress tracking and management
  - In the most recent third-party assessment, remediation of all 12 identified issues was completed in April 2026.

We continue to invest in these assessments as an important measure for protecting customer data.

8.3 Web Application Vulnerability Mitigation

The following vulnerability mitigation measures are implemented based on the IPA's "How to Build a Secure Website" and the OWASP Top 10.

Vulnerability	Mitigation
SQL Injection	Queries are constructed using parameter binding; user input is never directly concatenated into SQL statements
Cross-Site Scripting (XSS)	JSON API response design, security headers, and automatic escaping by the front-end framework
Cross-Site Request Forgery (CSRF)	Token-based stateless authentication and secure cookie attributes (Secure and SameSite)
OS Command Injection	No external commands are executed; all processing is completed within the application
Path Traversal	File paths are not specified directly; files are managed using cloud storage object keys

8.3 Web Application Vulnerability Mitigation

The following vulnerability mitigation measures are implemented based on the IPA's "How to Build a Secure Website" and the OWASP Top 10.

Vulnerability	Mitigation
Improper Session Management	Cryptographically secure token generation, appropriate expiration periods, and server-side token management
Clickjacking	Security headers are configured to deny framing
Broken Access Control	Role-based access control (RBAC) and workspace-level authorization checks

8.4 Input Validation

Multiple layers of validation are applied to all user input.

- **Request Validation:** Format and type checks, including email format, character limits, and required fields
- **Business Rule Validation:** Plan limits, resource existence, and permission checks
- **Database Constraints:** Final safeguards through integrity constraints such as NOT NULL, foreign keys, and unique constraints

8.5 Webhook Signature Verification

The authenticity of every webhook received from an external service is verified using cryptographic signatures.

LINE: Signature verification using a separate secret for each workspace
HubSpot: Signature verification, including timestamp validation to prevent replay attacks when using the latest signature method
Shopify: Signature verification using a timing-attack-resistant comparison method
Stripe: Signature verification built into the SDK
Klaviyo: Verification using a pre-shared secret, with a timing-attack-resistant comparison method

Requests that fail signature verification are rejected immediately. Paid uses a pull-based polling integration and therefore does not use webhooks.

8.6 Load Control and Availability Protection

- **Edge Protection:** All public endpoints are exposed through Cloudflare and protected against DDoS attacks
- **Asynchronous Processing:** Concurrency and dispatch rates are controlled for each job queue to maintain stability during traffic spikes
- **External API Calls:** Retry and backoff controls are implemented according to rate limits imposed by AI infrastructure and external services

8.7 Security Headers

The following security headers are explicitly added to all responses:

- **HTTP Strict Transport Security (HSTS):** Enforces HTTPS connections at all times.
- **X-Content-Type-Options (nosniff):** Prevents MIME type sniffing.
- **X-Frame-Options (DENY):** Prevents pages from being displayed within frames, protecting against clickjacking.
- **Referrer-Policy:** Controls the transmission of referrer information to external websites.

In addition, cache prevention controls are applied to responses containing sensitive data, such as authentication credentials.

8.8 Cross-Origin Resource Sharing (CORS)

Cross-origin access from browsers is disabled by default, and APIs are generally accessed through the same origin.

Only when cross-origin access is required are specific origins enabled through an explicit allowlist configured for each environment. Cross-origin requests with credentials are not permitted.

9. AI Security

AI inference and related processing are securely performed on Google Cloud's enterprise AI infrastructure. AI agents and customer data are also managed appropriately. This section describes security measures for AI and LLMs based on the OWASP Top 10 for LLM Applications 2025 framework.

9.1 AI Use Policy and Transparency

- **Purpose of Use:** Support for planning, executing, and analyzing marketing initiatives, and automated responses on LINE
- **Transparency:** AI-generated content is presented in a way that allows customers to recognize it as such
- **Human Oversight:** User approval is required for important actions such as message delivery and workflow creation

9.2.1 AI Models and Execution Platform

Lumo's AI agent capabilities are standardized on Gemini running on Google Cloud's Gemini Enterprise Agent Platform (formerly Vertex AI).

- **Provider:** Google (Gemini / Document AI)
- **Models:** Gemini is used for text generation, and Gemini embedding models are used to generate embeddings.
- **Use Cases:** Text generation, embedding generation, and document OCR (knowledge base features only; see the next page)
- **Processing Region:** All text generation and embedding generation performed by AI agents take place in the Google Cloud Tokyo region (asia-northeast1). Chat history, LINE user information, CRM integration data, and other data are not transferred outside Japan for AI processing.
- **Data Handling:** Governed by Google Cloud's enterprise data protection policies and Data Processing Agreement (DPA)
- **Closed Data Environment:** Related processing, including AI inference and document OCR, is completed within Google Cloud's enterprise infrastructure and is therefore protected under consistent security policies.

9.2.2 Customer-Enabled Optional Features

The following features operate only when explicitly enabled by the customer. They are disabled by default, and no external communication associated with these features occurs unless they are enabled.

- Web Search: A search API used by AI agents to access the latest information.
- External Agent Integration (A2A): A feature that integrates with external AI agents specified by the customer.

9.2.3 Processing Region for Document OCR (Document AI)

Of all AI-related processing, this is the only feature processed outside Japan.

- **Applicable Feature:** Limited to document OCR (text extraction) when customers upload PDF documents to the knowledge base.
- **Processing Region:** Currently processed in the Google Cloud Document AI U.S. region. We plan to migrate to the Japan region as soon as it becomes available.
- **Data Transmitted:** Only the contents of PDF files uploaded by customers to the knowledge base are processed by OCR. LINE users' personal data, chat histories, CRM integration data, and other data are not transmitted outside Japan for this processing.
- **Data Handling:** Data is processed only temporarily while OCR is performed and is not used to train AI models, in accordance with Google Cloud's enterprise data protection policies and Data Processing Agreement (DPA).
- **If Not Used:** This processing does not occur if no PDF documents are uploaded to the knowledge base. Content imported in formats other than PDF—including text, Markdown, CSV, Word documents, and web pages—is processed entirely within our proprietary processing infrastructure in Japan.

9.3 Handling of Customer Data

Data is managed separately for each contract and is not used to retrain external AI models.

- Customer data is never used to train or fine-tune AI models
- Input to AI models is limited to data from the relevant workspace
- AI processing results are stored only within the relevant workspace

9.4 Tenant-Level Data Isolation

- **Tenant Isolation for Vector Search (RAG)**: Workspace-level filters are always applied to search queries, ensuring that data from other tenants is not included in results
- **Document Storage Isolation:** Uploaded documents are stored separately for each workspace
- **Conversation History Isolation:** Conversation histories with AI agents are isolated by workspace

9.5.1 AI Agent Safety Design

Human-in-the-Loop (Human Approval Workflow)

AI agents require explicit user approval before performing high-impact actions.

Examples of actions requiring approval:

- Creating and scheduling LINE broadcast messages
- Creating and modifying segments
- Creating and activating workflows
- Creating A/B tests

These actions are classified according to their risk level. High-risk actions are executed only after the user has reviewed and approved them.

9.5.2 AI Agent Safety Design

Agent Permission Restrictions

- The actions available to each AI agent are explicitly defined, and agents cannot perform actions outside their defined scope.
- Customer agents are limited to the minimum operations necessary.
- A maximum number of conversation turns is set to prevent infinite loops.
-

Autonomy Controls (Trust Score)

For low-risk actions only, the scope of automated execution is adjusted according to a trust score based on past performance.

Sending broadcast messages and activating workflows always require user approval, regardless of the trust score. This requirement is never relaxed based on the trust score.

9.6 Prompt Injection Mitigation

- **Separation of System Instructions and User Input:** System instructions and user messages are structurally separated so that user input cannot interfere with system instructions
- **Action Parameter Validation:** Action parameters generated by AI must pass validation before execution
- **Structured Responses:** Action results are processed as structured data, preventing free-form text from directly affecting operations

9.7 Output Validation and Quality Management

- **Structured Action Results:** Results of actions performed by AI are processed as structured data
- **Secure Conversion of LINE Output:** Content for LINE messaging is converted into a secure format through a dedicated formatter
- **Customer Agent Safeguard:** Customers can disable AI-powered automated responses at any time using an automated-response stop flag

9.8 Rate Limiting and Resource Management

- **External API Rate Limit Handling:** Automatic retries and traffic control are implemented for calls to AI platform APIs.
- **Conversation Turn Limits:** A maximum number of agent conversation turns is configured to prevent excessive resource consumption.
- **Timeout Controls:** Appropriate timeouts are configured for external communications.

9.9 AI Quality and Safety Monitoring

- Telemetry related to the quality and safety of AI agents is designed to remain entirely within Google Cloud (Cloud Trace).
- Conversation content is not collected for quality evaluation and is not transmitted to external observability services.

10. LINE Integration Security

As a LINE marketing tool, integration with LINE Official Accounts is central to Lumo. As an LY Corporation Certified Technology Partner, we provide secure integrations that meet the LINE platform’s security requirements.

10.1 LY Corporation Certified Technology Partner

We are certified by LY Corporation as a technology partner for LINE Official Accounts. This certification requires compliance with LINE platform security requirements and successful completion of a technical review. Our implementation complies with the security checklist provided by LINE Developers.

10.2 Secure Webhook Reception

Webhooks from the LINE Platform are protected through cryptographic signature verification, and unauthorized requests are rejected.

- **Signature Verification:** Every webhook request is verified to exclude unauthorized requests originating outside the LINE Platform
- **Isolated Channel Secret Management:** A separate channel secret is used and encrypted for each workspace. A secret belonging to one workspace is never used to verify another workspace

10.3 Protection of LINE User Data

- **LINE ID Management:** LINE user IDs are managed on a per-workspace basis, with tenant isolation applied.
- **Profile Information:** Profile information obtained from LINE, such as display names and profile images, is accessible only within the applicable workspace.
- **Access Token Management:** LINE channel access tokens are stored in encrypted form.
- **End-User Data Deletion:** Functionality is provided to accommodate requests to delete the personal data of LINE users (end users).

10.4 Message Delivery Security

- **Pre-Delivery Approval Flow:** Messages created by AI agents are not sent until the user previews and approves them
- **Segment Delivery Validation:** Recipient segment conditions reference only workspace data, ensuring that messages are not delivered to users in other tenants
- **Secure Content Conversion:** Message content is converted through a dedicated formatter into a secure format that complies with LINE specifications

10.5 LINE Login

- **OAuth 2.0 / OpenID Connect Compliance:** LINE Login is implemented using standard OAuth 2.0 and OpenID Connect flows
- **End-User Consent:** When LINE Login is used, end users are shown a consent screen for the provision of information
- **Data Minimization:** Information obtained through LINE Login is limited to the minimum necessary to provide the service

11. Monitoring, Logging, and Incident Response

Lumo maintains continuous monitoring to ensure stable service operations and security. We have also established a framework for rapid response in the event of an incident.

11.1 Log Management and Audit Trails

- **Structured Logging:** Structured logs in JSON format are consolidated in a cloud-based log management platform.
- **Standard Fields:** Request IDs, user IDs, workspace IDs, and other standard fields are recorded automatically.
- **Distributed Tracing:** Request processing paths are traced, enabling issues to be identified quickly.
- **Protection of Personal Information:** Personal information, such as email addresses, is not recorded directly in logs. Only internal IDs are recorded.
- **Audit Log Retention:** Audit logs are retained in the production environment for one year. This retention period is enforced through Cloud Logging retention settings managed as Infrastructure as Code.
- **Data Access Audit Logs:** Data access audit logging is enabled for secret management (Secret Manager), access management (IAM), and databases (AlloyDB), providing an audit trail of privileged operations.

11.2 Monitoring and Alerts

- **Application Monitoring**: Continuous monitoring through dashboards, metrics, and alerts
- **Log Monitoring:** Error log detection and log-based alerts
- **Distributed Tracing:** Visualization of request processing paths and latency analysis
- **Availability Monitoring:** HTTP health checks for public services

11.3 Incident Response Procedures

Security incidents are handled according to the following procedures.

Phase	Details
1. Detection and Reporting	An incident is identified through a monitoring alert or a report from personnel. The person who discovers it immediately reports it to the security officer
2. Initial Response	Determine the scope of impact and decide whether to isolate or suspend services as necessary
3. Investigation and Analysis	Identify the cause and determine the affected data and users
4. Recovery	Restore normal system operations and recover data
5. Notification	Notify affected customers and report as required by law (see 11.4 for details)
6. Prevention of Recurrence	Address the root cause, review processes, and retain response records

11.4 Security Event Notification

- **Initial Customer Notification:** In the event of a security incident, affected customers will receive an initial notification within 72 hours.
- **Regulatory Reporting:** In the event of a personal data breach or similar incident, we will report it to the Personal Information Protection Commission in accordance with applicable laws and regulations. An initial report will be submitted within three to five days of becoming aware of the incident, followed by a final report within the legally prescribed timeframe—in principle, within 30 days, or within 60 days for incidents involving unauthorized access or similar circumstances.
- **Notification Methods:** Email, notifications within the administration interface, or both.
- **Notification Details:** Notifications will include an overview of the incident, its scope of impact, and recommended actions for customers.

12. Availability and Business Continuity

Data is continuously backed up automatically. Redundant architecture and disaster recovery mechanisms support stable delivery of the Lumo service.

12.1 Service Availability (SLA)

- **Target Availability:** 99.9% monthly
- **Service Hours:** 24 hours a day, 365 days a year
- **Availability Calculation:** Excludes scheduled maintenance

12.2 Redundancy and Auto Scaling

- Core services run continuously across multiple instances to eliminate single points of failure
- Instances scale out automatically as traffic increases
- Minimum instance settings minimize the impact of cold starts

12.3 Backup and Disaster Recovery (DR)

- **Automated Backups:** Weekly full backups and continuous backups using point-in-time recovery (PITR) enable restoration to any point in time.
- **Production Environment Deletion Protection:** Database deletion protection is enabled to prevent accidental deletion.
- **RTO:** Less than 1 hour
- **RPO:** Less than 5 minutes

12.4 Scheduled Maintenance

- Customers are notified in advance when scheduled maintenance is required
- **Notice Period:** In principle, at least five business days in advance; for emergencies, notice is provided as early as possible
- Rolling deployments are used whenever possible to avoid service interruption

13. External Service Integration Security

In addition to LINE Official Accounts, Lumo integrates with HubSpot, Shopify, Klaviyo, Stripe, and Paid to support customer marketing activities. All communications with integrated services are encrypted, and authentication credentials are securely managed. For LINE integration security, see Section 10, LINE Integration Security.

13.1 External Services Used

Category	Service	Purpose
Messaging	LINE Platform	Message delivery, webhook reception, and LINE Login (see Section 10 for details)
CRM	HubSpot	Contact synchronization and workflow integration
EC	Shopify	Customer and order data synchronization
Marketing	Klaviyo	Segment and campaign integration
Payments (Cards)	Stripe	Credit card payments and subscription management
Payments (Bank Transfer)	Paid	Bank transfer and invoice payments

13.1 External Services Used

Category	Service	Purpose
Email	SendGrid	Transactional email delivery
AI	Google Cloud AI（Gemini Enterprise Agent Platform /Document AI）	Text generation, embedding generation, and document OCR (OCR applies only to PDF documents used in the knowledge base feature; see Chapter 9 for details)
Help	Zendesk	Help center integration

13.2 CRM Integrations（HubSpot / Shopify / Klaviyo）

- **OAuth 2.0 Authentication:** OAuth 2.0 is used to authenticate with each CRM service, and access tokens are securely managed
- **Encrypted Token Storage:** OAuth tokens are encrypted at the application level
- **Webhook Signature Verification:** Signatures are verified for webhooks from each service
- **HubSpot Certified Technology Partner:** Compliant with HubSpot’s security and privacy standards
- **GDPR Webhook Support:** Supports mandatory GDPR webhooks from HubSpot and Shopify, including customer data deletion requests
- **Integration Token Reauthentication Safeguard:** If the authorization token for an external service is detected as expired, the applicable integration is securely suspended and the customer is prompted to reauthenticate (reconnect). This prevents processing from continuing with an expired token.

13.3 Payment Integrations (Stripe / Paid)

Stripe (Credit Card Payments)

- **PCI DSS Compliance:** Card information is processed directly by Stripe and does not pass through our systems
- **Webhook Signature Verification:** Uses signature verification built into the SDK
- **Secret Management:** Authentication credentials are managed in GCP Secret Manager

Paid (Bank Transfer / Invoice Payments)

- **Credential Management:** Uses authentication credentials managed in GCP Secret Manager
- **Communication Encryption:** All API communications are encrypted using HTTPS/TLS
- **Tenant Isolation:** Payment data is tenant-isolated through billing agreements associated with each workspace

13.4 Communication Security with External Services

- TLS Encryption for All Communications: All communications with external services are encrypted using TLS 1.2 or later
- Centralized Secret Management: Authentication credentials for all external services are managed in GCP Secret Manager
- Keyless Authentication: The deployment process does not use long-lived keys
- Event-Driven Architecture: Receipt and processing of external events are separated to prevent failures in an external service from affecting the entire system

14. Customer-Facing Security Features

Lumo allows customers to customize their own security settings.

14.1 Available Security Settings

The following security features can be configured from the admin console.

Feature	Description
Two-Factor Authentication (2FA)	Two-factor authentication using one-time passwords can be enabled for each account
Member Permission Management	Roles (Administrator / Member) and detailed permissions can be configured for each workspace member
API Key Management	API keys can be issued and revoked from the admin console
AI Automated Response Controls	Customer Agent automated responses can be disabled for individual users
AI Agent Action Approval	Approval is required before the Marketing Agent performs high-risk actions

14.2 Recommended Security Settings

For more secure use of Lumo, we recommend the following settings.

1. **Enable Two-Factor Authentication:** Enable two-factor authentication for all users
2. **Principle of Least Privilege:** Grant members only the minimum permissions required for their work
3. **Regular API Key Updates:** Rotate API keys regularly
4. **Remove Unnecessary Members:** Promptly remove members who no longer require access due to departure, transfer, or other reasons
5. **Regular Password Changes:** Regular password changes are recommended

Appendix A.
Compliance Framework Mapping

Ministry of Economy, Trade and Industry (METI)「Cloud Service Level Checklist」

Category	Relevant Sections
Availability	12.1 Service Availability; 12.2 Redundancy
Reliability	6.5 Backup and Recovery; 11.3 Incident Response
Performance	12.2 Redundancy and Auto Scaling
Scalability	12.2 Redundancy and Auto Scaling
Support	11.3 Incident Response; 11.4 Security Event Notification
Data Management	Sections 6.1–6.7, Data Protection
Security	2.3 Certifications and Accreditations; 2.4 External Assessments; Sections 5–9

Ministry of Internal Affairs and Communications (MIC)「ASP/SaaS Information Disclosure Guidelines」

Category	Relevant Sections
Business Operations	2.2 Company Information
Personnel	4.3 Security Education
Compliance	4.6 Legal and Regulatory Compliance
Service Characteristics	2.1 Service Overview
Application	8. Application Security
Network	5.2 Network Security、5.3 Edge Security
Data Center	5.1 Cloud Infrastructure
ServiceSupport	11.3 Incident Response; 12.4 Scheduled Maintenance
AI-Related	9. AI Security

IPA「How to Build a Secure Website」

VulnerabilityCategory	Relevant Sections
SQL Injection	8.3
OS Command Injection	8.3
Path Traversal	8.3
Improper Session Management	7.4、8.3
XSS	8.3
CSRF	8.3
HTTP Header Injection	8.3
Clickjacking	8.3、8.7
Broken Access Control	7.5、8.3

OWASP Top 10 for LLM Applications 2025

Item	Relevant Sections
LLM01: Prompt Injection	9.6
LLM02: Sensitive Information Disclosure	9.3、9.4
LLM03: Supply Chain	9.2
LLM04: Data and Model Poisoning	9.3、9.4
LLM05: Improper Output Handling	9.7
LLM06: Excessive Agency	9.5
LLM07: System Prompt Leakage	9.6
LLM08: Vector and Embedding Weaknesses	9.4
LLM09: Misinformation	9.7
LLM10: Unbounded Consumption	9.8

Appendix B. External Cloud Services Used

Appendix B. External Cloud Services Used

Service	Provider	Purpose	Data Location
Google Cloud Platform	Google LLC	Application infrastructure, databases, AI infrastructure (Gemini Enterprise Agent Platform), and document OCR	Japan (Tokyo region). Only document OCR (Document AI) for PDF documents used in the knowledge base feature is processed in the United States (see Section 9.2.3).
Cloudflare	Cloudflare, Inc.	CDN、DDoS Protection、TLS Termination、File Storage	Global (edge) / Asia-Pacific (storage)
LINE Platform	LY Corporation	Messaging integration	Japan
HubSpot	HubSpot, Inc.	CRM Integrations	United States
Shopify	Shopify Inc.	E-commerce integration	Canada / United States
Klaviyo	Klaviyo, Inc.	Marketing integration	United States

Appendix B. External Cloud Services Used

Service	Provider	Purpose	Data Location
Stripe	Stripe, Inc.	Credit card payments	United States
Paid	RACCOON FINANCIAL, Inc.	Bank transfer payments	Japan
SendGrid	Twilio Inc.	Email delivery	United States
Zendesk	Zendesk, Inc.	Help center	United States

Appendix C. Contact Information

Appendix C. Contact Information

For security-related inquiries, please contact us at the address below.

Item	Details
Contact	SecurityContact（Little Help Agency LLC）
Email Address	hq@littlehelp.co.jp
Business Hours	Weekdays, 10:00–18:00 (Japan Standard Time)

Reports of vulnerabilities and security incidents are also accepted through the contact above.

Related Documents

- Lumo Terms of Service
- Data Processing Agreement (Agreement on the Handling of Personal Information)
- Privacy Policy

LITTLE HELP AGENCY

Little Help Agency LLC

xLINK, 3F Shin-Otemachi Building, 2-2-1 Otemachi, Chiyoda-ku,
Tokyo 100-0004, Japan

https://www.lumo.cx/en/