

Customer Engagement Platform

API Usage Policy

REFERENCE DOCUMENT

Version 1.0 | July 2026

1. Purpose & Scope

This API Usage Policy (“Policy”) governs the access to and use of the jrni REST API (“API”) by any party (“Client”) that enters into a Master Services Agreement, Subscription Agreement, or similar contractual arrangement with jrni Inc. (“jrni”). This Policy is incorporated by reference into such agreements and sets forth the permitted usage parameters, rate limits, fair use obligations, and enforcement procedures applicable to all API integrations.

This Policy applies to all API tiers — Public, Member, and Admin — as defined in the jrni Developer Documentation (dev.jrni.com) and covers the following API surfaces:

> ℹ️ **Note:**
> This Policy covers direct API interactions only.

2. API Permission Tiers

The jrni API is organized into three permission tiers. Each tier carries distinct authentication requirements, data access scope, and rate limit parameters. Clients must ensure their integration credentials are scoped to the minimum necessary permission tier for their use case.

Tier	Primary Use Case	Authentication	Typical Consumer
Public	Customer-facing scheduling journeys — browsing services, availability, and creating bookings via baskets	App ID + App Key (no user auth)	Website widgets, mobile apps, self-service kiosks
Member	Authenticated customer interfaces — viewing/modifying existing bookings, updating customer profile data	Auth Token (customer session)	Customer portals, post-booking management screens
Admin	Staff and back-office operations — full account management, reporting, bulk operations, configuration	Auth Token (admin session) or OAuth 2.0	CRM integrations, analytics pipelines, workforce tools

Clients are prohibited from using Admin-tier credentials for Public-tier use cases (e.g., high-volume customer-facing booking flows). Misuse of elevated credentials could be subject to immediate suspension per Section 8.

3. Rate Limits & Throttling

3.1 Standard Rate Limits

Rate limits are enforced per API key / auth token, per API tier, and per rolling time window. The following standard limits apply unless otherwise agreed in writing:

Tier	Requests / Second (Burst)	Requests / Minute	Requests / Hour	Requests / Day
Public API	10	300	5,000	50,000
Member API	5	150	2,500	25,000
Admin API	5	120	2,000	20,000

3.2 Pagination & Page Size

All list endpoints return a maximum of 30 records per page by default. Clients may request up to 100 records per page using the per_page parameter. Requests for per_page values exceeding 100 will be capped at 100 and do not consume additional rate limit quota.

- Default page size: 30 records
- Maximum page size: 100 records (per_page=100)
- Pagination is cursor-based via page and per_page URL parameters
- HAL-compliant _links.next and _links.previous are provided in paginated responses

> ⚠️ **Important:**
> Persistent 429 violations — particularly those that suggest automated attempts to circumvent rate limits — may result in API key suspension and are subject to the enforcement provisions in Section 8 of this Policy.

3.3 High-Volume & Enterprise Rate Limit Tiers

Clients with documented requirements exceeding the standard limits set out in Section 3.1 may request elevated rate limit tiers. Such requests must be submitted in writing to jrni Customer Success and are subject to:

- Technical review of the Client's integration architecture
- Confirmation of use case legitimacy and business justification
- Potential adjustment to subscription pricing
- A written addendum to the governing contract specifying the elevated limits

4. Authentication & Credential Management

4.1 Supported Authentication Methods

jrni supports the following authentication methods. The appropriate method depends on the integration type and the API tier being accessed:

Method	Use Case	Token Expiry
App ID + App Key	Server-to-server Public API calls; no user session required	Non-expiring (rotate periodically)
Auth Token (session)	Member and Admin tier calls tied to a user session	Configurable; default ~24 hours
OAuth 2.0	Third-party integrations requiring delegated access on behalf of a user	Access token ~1 hr; refresh token per grant

4.2 Credential Security Obligations

Clients are responsible for securing all API credentials issued by jrni. Clients must:

- Store API keys, tokens, and secrets in secrets managers or encrypted vault services — never in source code, version control, or client-side JavaScript
- Rotate App Keys at least every 12 months or immediately upon suspected compromise
- Revoke and re-issue credentials immediately when personnel with access depart
- Use separate credentials per environment (production, staging, development)
- Never share credentials across multiple Clients or sub-contractors without express written consent from jrni

jrni is not liable for unauthorized access or data breaches resulting from Client failure to comply with these credential security obligations.

4.3 Token Expiry & Session Management

Auth tokens expire after the configured period (default 24 hours). Clients must implement token refresh logic and gracefully handle HTTP 401 Unauthorized responses by re-authenticating rather than surfacing errors to end users. Session tokens for customer-facing (Member) flows should be treated as short-lived and scoped to a single user session.

6. Acceptable Use

6.1 Permitted Uses

The jrni API may only be used for purposes directly related to the Client's authorized business activities as described in the governing contract. Permitted uses include:

- Building customer-facing booking, queuing, and event registration journeys
- Integrating jrni scheduling data with the Client's CRM, ERP, or workforce management systems
- Extracting analytics and reporting data for internal business intelligence purposes
- Automating appointment and event management workflows for operational efficiency
- Bulk import of staff, locations, services, and schedules during onboarding or migration

6.2 Prohibited Uses

The following activities are strictly prohibited and may result in immediate suspension of API access:

- Scraping jrni data for commercial resale, competitive intelligence, or unauthorized data aggregation
- Reverse engineering, decompiling, or attempting to circumvent jrni's security controls
- Using the API to access data belonging to another jrni client without authorization
- Automating the creation of fraudulent bookings, phantom accounts, or spam registrations
- Deliberately exceeding rate limits to test platform resilience without prior written approval
- Using Admin-tier credentials in public-facing or unauthenticated environments
- Storing or transmitting API credentials in client-side code, public repositories, or unencrypted storage

6.3 Fair Use Principle

Even within the rate limits set out in Section 3, Clients are expected to use the API efficiently and in good faith. This includes:

- Caching responses where appropriate to avoid redundant API calls (e.g., service lists, company configurations)
- Using webhook-driven architectures where real-time event notification is available, rather than polling
- Scheduling batch/bulk operations during off-peak hours (outside 08:00–20:00 local business time)
- Implementing request queuing on the Client side to smooth traffic distribution

6.4 Client Responsibilities

Client Responsibilities for Public-Facing Application Security

Clients who expose jrni APIs through publicly accessible applications are solely responsible for implementing appropriate security controls to protect those endpoints from abuse, spam, and unauthorised access. This includes, but is not limited to, the following measures:

Web Application Firewall (WAF)
Clients must deploy a WAF in front of any public-facing application that consumes jrni APIs. The WAF must be configured to detect and mitigate common threat vectors including, but not limited to, SQL injection, cross-site scripting (XSS), and automated bot traffic.

Bot and Spam Prevention
Clients must implement bot mitigation controls on all public-facing booking flows, registration forms, and API entry points. Acceptable controls include CAPTCHA or reCAPTCHA challenges, rate limiting, IP throttling, and behavioural analysis tooling. Controls must be reviewed periodically to ensure they remain effective against evolving automated threats.

One-Time Password (OTP) Verification
Where jrni's integrated OTP functionality is available, clients are strongly encouraged to enable it as part of their customer-facing booking and registration journeys. OTP verification reduces fraudulent bookings, appointment spam, and the submission of invalid contact data — protecting both the client's operational data integrity and jrni's underlying platform infrastructure.

General Obligation
jrni provides a secure and reliable API platform; however, jrni accepts no liability for abuse, data integrity issues, or service disruption arising from a client's failure to implement adequate security controls on their public-facing applications. Clients are expected to follow industry best practices and comply with all applicable security standards relevant to their sector (including, where applicable, PCI-DSS, ISO 27001, and relevant financial services regulatory requirements).

7. Data Governance & Privacy

All data accessed through the jrni API, including personally identifiable information (PII) of customers and staff, is subject to the data processing provisions of the governing contract and jrni's Data Processing Agreement (DPA).

7.1 Data Minimization

Clients must request only the data fields necessary for their stated integration purpose. The use of broad, undifferentiated queries to extract complete customer datasets without a documented business need is a violation of this Policy.

7.2 Data Retention

API responses containing personal data must not be retained by Client systems beyond the period necessary for the stated processing purpose. Retention schedules must align with the Client's data retention policy and applicable regulations (GDPR, CCPA, etc.).

7.3 Data Breach Notification

If a Client suspects or confirms that API credentials have been compromised or that jrni customer data has been exposed through the Client's integration, the Client must notify jrni Security (security@jrni.com) within 24 hours of discovery.

> 🔒 **Security Contact:**
> Report credential compromise or suspected data exposure to: security@jrni.com For non-urgent API support: support@jrni.com or via the jrni Help Portal at jrnisupport.helpdocs.io

8. Enforcement & Remediation

8.1 Monitoring

jrni continuously monitors API usage patterns for anomalies including, but not limited to, sustained rate limit breaches, unusual data access volumes, authentication failures, and access pattern deviations. Clients consent to this monitoring as a condition of API access.

8.2 Graduated Enforcement

Where jrni identifies a Policy violation, the following graduated response applies:

Severity	Trigger	jrni Action	Resolution Path
Low	Occasional 429 spikes; minor pagination misuse	Automated throttling; advisory notification to Client technical contact	Client self-remediation within 14 days
Medium	Sustained rate limit abuse; incorrect credential tier usage; webhook ACK failures >20%	Temporary API key suspension (up to 72 hours); written notice to Client	Client provides remediation plan within 7 days
High	Prohibited use; credential exposure; data scraping; circumvention attempts	Immediate API key revocation; escalation to account management	Contract review; reinstatement at jrni's discretion
Critical	Breach of data protection obligations; unauthorized data access; security incident	Immediate suspension; legal escalation; DPA breach notification	Governed by contract and applicable law

8.3 Client Remediation Obligations

Upon receipt of a Medium or High severity notice, the Client must:

- Acknowledge receipt within 24 hours
- Provide a written root-cause analysis within 5 business days
- Implement and document corrective technical controls
- Confirm remediation to jrni Customer Success in writing before API access is restored

9. Policy Amendments

jrni reserves the right to amend this Policy at any time. Material changes — defined as modifications to rate limits, permitted uses, or enforcement procedures and posted to dev.jrni.com.