 Generate a policy for API rate limiting.

A good API rate limiting policy protects your API from abuse, ensures fair usage among all users, and maintains high availability and performance.

**API Rate Limiting Policy 🚀**

This policy outlines the rate limits for accessing our API. These limits are in place to ensure fair usage, prevent abuse, and maintain a high-quality, responsive service for all our users.

**Guiding Principles 🎯**

* Stability & Reliability: Protect the underlying infrastructure from being overwhelmed by too many requests.
* Fair Usage: Ensure that all clients have equitable access to API resources.
* Security: Mitigate certain types of attacks, such as DDoS and brute-force attempts.

**Rate Limits ⏱️**

Our API employs a tiered approach to rate limiting, with different limits based on the type of API key or user plan. Limits are typically measured by the number of requests per second (RPS) or requests per minute (RPM) to specific endpoints or globally across the API.

General Guidelines:

* Anonymous/Trial Users:
  + Limit: 10 requests per minute (RPM)
  + Scope: Global (across all endpoints)
* Basic/Free Tier Users:
  + Limit: 60 requests per minute (RPM)
  + Scope: Global (across all endpoints)
* Premium/Paid Tier Users:
  + Limit: 300 requests per minute (RPM) or higher, as per specific plan details.
  + Scope: May include higher global limits and/or specific per-endpoint limits.
* Enterprise Clients:
  + Limit: Custom limits based on negotiated agreements.
  + Scope: Custom.

Specific Endpoint Considerations:

Certain computationally intensive or sensitive endpoints may have stricter, independent rate limits. These will be documented in the specific API documentation for those endpoints.

Bursting:

We allow for short bursts of requests exceeding the defined limits for a brief period, provided the overall average remains within the allocated quota. Consistent bursting that exceeds limits will be treated as a violation.

**Exceeding Limits 🚦**

When a client exceeds the defined rate limits, the API will respond with an HTTP 429 Too Many Requests status code.

The response headers will typically include information about the violated limit and when the client can retry the request. Common headers include:

* Retry-After: The number of seconds to wait before making a new request.
* X-RateLimit-Limit: The current rate limit.
* X-RateLimit-Remaining: The number of requests remaining in the current window.
* X-RateLimit-Reset: The time (in UTC epoch seconds)1 when the current window resets.

Consequences:

* Temporary Throttling: Requests will be temporarily blocked.
* Repeated Violations: Consistent abuse of rate limits may lead to temporary suspension of API access or, in severe cases, permanent revocation of API keys. We will attempt to contact the account holder before taking more severe actions.

**Best Practices for Consumers 👍**

* Efficient Coding: Optimize your API calls. Cache responses where appropriate and avoid making redundant requests.
* Retry Logic: Implement proper retry mechanisms in your application that respect the Retry-After header. Use exponential backoff strategies for retries.
* Monitor Usage: Keep an eye on your API usage through your dashboard (if available) or by monitoring response headers.
* Plan Ahead: If you anticipate a significant increase in usage, please contact our support team in advance to discuss potential adjustments to your rate limits.

**Requesting Higher Limits 📈**

If your application requires higher rate limits than those provided by your current plan, please contact our support team or your account manager. Requests will be evaluated based on:

* Your current usage patterns.
* The justification for the increase.
* Your subscription tier.

**Policy Updates 🔄**

This API Rate Limiting Policy is subject to change. We will notify users of any significant changes through email or by posting an update on our developer portal. We encourage you to review this policy periodically.

**Contact Us 📧**

If you have any questions or concerns regarding this policy or your API usage, please contact our support team.