Generate a policy for API rate limiting.

**API Rate Limiting Policy**

**1. Purpose**

The purpose of this policy is to ensure the stability, availability, and fair usage of our API services. Rate limiting helps prevent abuse, reduces the risk of service degradation, and ensures a consistent experience for all users.

**2. Scope**

This policy applies to all users and applications accessing our API services.

**3. Rate Limits**

* **Requests per Minute**: Each API key is limited to 100 requests per minute.
* **Requests per Hour**: Each API key is limited to 1,000 requests per hour.
* **Requests per Day**: Each API key is limited to 10,000 requests per day.

**4. Rate Limit Headers**

The API will include the following headers in responses to inform clients about their rate limit status:

* **X-RateLimit-Limit**: The maximum number of requests allowed in the current window.
* **X-RateLimit-Remaining**: The number of requests remaining in the current window.
* **X-RateLimit-Reset**: The time at which the current rate limit window resets.

**5. Exceeding Rate Limits**

* When a client exceeds the rate limit, the API will return an HTTP 429 (Too Many Requests) status code.
* The response will include a **Retry-After** header indicating the time (in seconds) the client should wait before making another request.

**6. Monitoring and Enforcement**

* API usage will be monitored in real-time to detect and prevent abuse.
* Automated systems will enforce rate limits and take appropriate action, such as temporarily blocking API keys that consistently exceed limits.

**7. Exceptions**

* Special rate limits may be negotiated for high-volume users or enterprise clients. Contact our support team to discuss custom rate limits.

**8. Review and Updates**

* This policy will be reviewed periodically to ensure it meets the needs of our users and the performance requirements of our API.
* Updates to the policy will be communicated to users in advance.

**9. Contact Information**

For questions or concerns about this policy, please contact our support team at [support email].

**Implementation Notes**

* **API Gateway**: Use an API gateway to enforce rate limits and monitor usage.
* **Logging**: Maintain logs of API requests to analyze usage patterns and detect anomalies.
* **Documentation**: Clearly document the rate limiting policy in your API documentation to inform users.