**Third-Party API Disclosure Policy – Destination Vista**

**Purpose of the Policy**

The **Third-Party API Disclosure Policy** explains how **Destination Vista** integrates with third-party APIs to enhance platform features, manage vendor data, facilitate payments, location services, and deliver a seamless user experience. This policy ensures transparency, regulatory compliance, and security in all external API communications.

**1. What is a Third-Party API Integration?**

Third-party APIs (Application Programming Interfaces) are external services and tools integrated into **Destination Vista** for specific functions such as:

* Payment processing
* Location mapping
* Weather data
* Booking verification
* Travel insights
* Government tourism APIs (where applicable)

**2. Types of Third-Party APIs Used**

Destination Vista may use the following categories of third-party APIs:

**a. Payment & Transaction APIs**

* Used for processing secure payments and refunds (e.g., Razorpay, PayU, Stripe)
* Ensures PCI-DSS compliance and secure encryption standards

**b. Map & Location Services**

* Google Maps API or OpenStreetMap API
* Used to provide interactive maps, directions, and route-based tour planning

**c. Authentication & Security APIs**

* Google/Facebook login APIs (if social login is enabled)
* OTP verification via SMS gateways (e.g., Twilio, Msg91)

**d. Travel Data APIs**

* Weather APIs for trip planning
* Government or public tourism board APIs for official data (state tourism APIs)

**e. Analytics & Tracking APIs**

* Google Analytics, Facebook Pixel for usage behavior (strictly anonymized)
* Used to improve website performance, not to track personally identifiable information without consent

**f. Email & Notification APIs**

* Mailgun, SendGrid, or similar tools for newsletter delivery
* Push notifications (Firebase Cloud Messaging)

**3. Data Shared with Third-Party APIs**

* Only **minimum required data** is shared for the specific function.
* All integrations use **secure HTTPS endpoints**.
* Sensitive user data (like passwords or financial details) is never shared unless encrypted and legally required.
* All vendors and APIs comply with **Indian IT Act, 2000**, and **Data Protection Bill, 2023**.

**4. Vendor API Use Restrictions**

* API keys provided to vendors (for managing their dashboards or listings) must not be shared.
* Misuse or abuse of APIs will result in immediate **account suspension** and legal action.
* APIs provided to vendors are monitored with **rate limits** and access logs.

**5. User Rights & Transparency**

* All users have the right to request information about how their data is used with third-party APIs.
* Users can request API-related disclosures via:  
  📧 **privacy@destinationvista.in**

**6. Policy Review & Update**

* This policy is reviewed **quarterly** or upon integration of any **new third-party API**.
* Major changes to API data flow will be notified to users via email and posted on the platform.

**7. Contact for API-related Inquiries**

For concerns or queries related to API integrations:  
📧 **api@destinationvista.in**  
📞 **+91-XXXXXXXXXX**