Developer Profile

Developer Profile collects your organization's contact information, information about the data you require in Amazon Services APIs, and security and use information to ensure your compliance with Amazon's Acceptable Use Policy and Data Protection Policy. If you are an Amazon Marketplace Web Service developer with multiple developer IDs, you do not need to submit a separate Developer Profile for each developer ID.

Once you complete the Developer Profile, Amazon will evaluate your information and create a case with next steps. You may be asked to provide additional information or documentation, so please complete all fields truthfully and accurately.

Contact Information

Organization name

INSPIRING INFOSYS

Organization website

https://inspiringinfosys.com/

Organization home country

India

Primary contact name

Maqsood Alam Ansari

Contact email

info@inspiringinfosys.com

Contact country code

+91

Contact phone number

8444040514

Data Access

Please select the option that best describes your organization

Note that your answers represent your organization. Need more information?

Public Developer: I build and offer publicly available applications that are used by other compa

If you are currently a developer, please provide your organization's developer ID(s)

Please include all of your organization's developer IDs separated by a comma. Note: If you are an Amazon Marketplace Web Service developer with multiple developer IDs, you do not need to submit a separate Developer Profile for each developer ID.

703751142833

Roles

Roles determine access to Selling Partner API. Role definitions can be found here
Note: Restricted roles contain Personally Identifiable Information (PII) about Amazon Buyers, and you will be required to provide additional information about your data use and security controls.

- [ ] Product Listing
  Create and manage product listings, including A+ content
- [ ] Pricing
  Determine list prices and automate product pricing.
- [ ] Amazon Fulfillment
  Ship to Amazon, and Amazon ships directly to customer. Includes Fulfillment by Amazon.
- [ ] Buyer Communication
  Manage messaging to and from Amazon buyers.
- [ ] Buyer Solicitation
  Solicit Amazon buyers for feedback.
- [ ] Selling Partner Insights
  View information about the Amazon Selling Partner account and performance.
- [ ] Finance and Accounting
  Produce account and financial statements. Does not include information required to generate tax invoices.
- [ ] Inventory and Order Tracking
  Analyze and manage inventory. Does not include information required to generate shipping labels.
- [ ] Sustainability Certification
  View and submit product sustainability certifications.
- [ ] Amazon Logistics
  Leverage Amazon as a shipping service.
- [ ] Business Product Catalog
  Search Amazon's business catalog
- [ ] Amazon Warehousing and Distribution
  Analyze and manage AWD shipments and inventory. Generally used for interacting with AWD inventory information and shipment details.
- [ ] Brand Analytics
  Access your sales and inventory data to manage your Amazon Retail business.
- [ ] Business Purchase Reconciliation
  View Amazon Business purchases to reconcile payments with orders.
- [ ] Amazon Business Analytics
  Access Amazon Business Analytics Reports
- [ ] Amazon Business Order Placement
  Used for automating Amazon Business orders and checkout
- [ ] Account Information Service Provider

Account information Open Banking APIs for licensed Third Party Providers (TPPs) in Europe

- [ ] Payment Initiation Service Provider
  Initiation of payments Open Banking APIs for licensed Third Party Providers (TPPs) in Europe
- [ ] Direct-to-Consumer Shipping (Restricted)
  Generate shipping labels and ship Amazon orders directly to customers.
- [ ] Tax Invoicing (Restricted)
  Generate tax invoices to comply with tax regulation.
- [ ] Tax Remittance (Restricted)
  Calculate and remit sales taxes.
- [ ] Professional Services (Restricted)
  Provide add-on services such as Room of Choice Delivery, Assembly and Installation to Amazon buyers.

App Integrations NEW

Opt-in App Integrations will allow your app to integrate onto Seller Central. See more details here.

- [ ] Notifications in Seller Central
  Allow app notifications to appear in Appstore and be linked from Seller Central.

Use Cases

Which marketplaces do you intend to support?

North America

- [ ] US
- [ ] Canada
- [ ] Mexico

South America

- [ ] Brazil

Europe

- [ ] France
- [ ] Germany
- [ ] Italy
- [ ] Spain
- [ ] Netherlands
- [ ] UK
- [ ] Ireland

Middle East

- [ ] UAE
- [ ] Egypt
- [ ] Saudi Arabia

Asia

- [ ] China
- [ ] Japan
- [ ] Singapore

India

- [ ] India

- [ ] Belgium
- [ ] Poland
- [ ] Sweden
- [ ] Turkey
- [ ] South Africa

Australia

- [ ] Australia

Describe the application or feature(s) you intend to build using the functionality in the requested roles.

We here trying to build an automation services for amazon sellers who are selling their products on amazon.in where they can fetch all amazon data using API such as product listing, inventory ,pricing to our website and we will set all thing in automation so that on on click they

Describe why you require Personally Identifiable Information to build your application or feature.

functionality, such as processing orders, generating reports, and managing seller tasks. PII like names, contact details, and order-related information is used solely to associate transactions with the correct sellers and customers, ensuring accurate order management and communication. No additional PII is collected beyond what is necessary for these operational

Describe how your application or feature(s) will benefit authorized users.

send emails to buyers.3. ASIN MAPPING Hijack Alert You will get notified if any other seller infiltrates in your listing. To avoid sales drop, Hijack play a key role to monitor and alert you. Designed for Amazon SPN and ATES

Do you support online merchants today?

Between 25 and 100

List the online channels that you support today

Sellwell CMS currently supports the following online sales channels:

Amazon

How many employees does your organization have?

Less than 25

Do you intend to launch functionality requiring Personally Identifiable Information (PII) within 90 days?

- ◯ Yes
- ◯ No

What differentiates your new feature/application from others applications in the category?

a single platform. Unlike other applications, it supports multiple channels (Amazon, Flipkart, Shopify, WooCommerce, Myntra) simultaneously, provides real-time inventory and order tracking, and enforces strong security and data encryption. Its intuitive dashboard, automation features, and robust analytics empower sellers to manage operations efficiently from one

Please describe any country-specific functionality that you provide.

Localization features such as INR currency support and regional date formats.

Integration with Indian logistics and courier services for accurate shipping and tracking.

Please list the Amazon programs you intend to support through your application or functionality.

Amazon Marketplace Web Service (MWS) / Selling Partner API (SP-API) – for automated order processing, reporting, and task management.

Security Controls

Do you use network controls to prevent unauthorized access to Amazon Information?

- ◯ Yes
- ◯ No

Do you restrict access to Amazon Information based on users' job duties or business functions?

- ◯ Yes
- ◯ No

Do you encrypt Amazon Information in transit?

- ◯ Yes
- ◯ No

Do you have an incident response plan that covers monitoring, detection, and response for potential threats and Security Incidents?

- ◯ Yes
- ◯ No

Does your incident response plan include reporting security incidents involving Amazon Information to security@amazon.com?

- ◯ Yes
- ◯ No

Are minimum password requirements established for personnel and systems?

- ◯ Yes
- ◯ No

Are credentials (passwords, encryption keys, secret access keys) stored securely? In other words, you avoid keeping credentials in public repositories, sharing credentials, or hard coding credentials into applications.

- ◯ Yes
- ◯ No

List all outside parties with whom your organization shares Amazon Information and describe how your organization shares this information.

We INSPIRING INFOSYS does not share any information with outside parties. We access amazon sellers data and provided them a dashboard to manage their daily basis manual task into automation

List all non-Amazon MWS sources where you retrieve Amazon Information.

We INSPIRING INFOSYS only relies on MWS to retrieve Amazon Information

Because the roles you have requested are Restricted, you must comply with the Personally Identifiable Information security requirements in the Data Protection Policy.

How long do you retain Personally Identifiable Information data?

- ◯ Less than 31 days after order shipments
- ◯ 31 to 90 days after order shipments
- ◯ 91 to 180 days after order shipments
- ◯ More than 180 days after order shipments

Do you have a privacy and data handling policy?

- ◯ Yes
- ◯ No

Do you encrypt Personally Identifiable Information at rest?

- ◯ Yes
- ◯ No

Do you use fine-grained access controls to restrict to Personally Identifiable Information?

- ◯ Yes
- ◯ No

Do you use audit logs to detect and alert on Security Incidents?

- ◯ Yes

- ◯ No

Are application changes evaluated in a dedicated test environment before pushing to production?

- ◯ Yes
- ◯ No

Do you conduct routine checks (e.g. through vulnerability scanning or penetration tests) of the application and network components (including hardware) that interact with PII at least every 180 days?

- ◯ Yes
- ◯ No

Do you scan application code for vulnerabilities prior to each release?

- ◯ Yes
- ◯ No

Do you have a formal change management process which defines responsibilities for testing, verifying, and approving changes, and restricts access to who may perform these actions?

- ◯ Yes
- ◯ No

Describe the network protection controls used by your organization to restrict public access to databases, file servers, and desktop/developer endpoints.

access to databases and file servers. All data is encrypted in transit (TLS 1.2+) and at rest (AES-256). Access is limited to backend servers and authorized users via VPN or IAM roles. S3 buckets block public access, and developer endpoints use MFA, VPN, and endpoint protection. Continuous monitoring and logging ensure secure, auditable access.

Describe how your organization individually identifies employees who have access to Amazon Information, and restricts employee access to Amazon information on a need- to-know basis.

Access to Amazon Information is strictly limited. No employees have direct access to customer or confidential data. All data is encrypted in transit and at rest using AWS KMS. Only essential order details are accessible to authorized system components for processing. Employee access is role-based, logged, and reviewed periodically to ensure least-privilege access.

Describe the mechanism your organization has in place to monitor and prevent Amazon Information from being accessed from employee personal devices (such as USB flash drives, cellphones) and how are you alerted in the event such incidents occur.

or transferred to personal devices. System architecture disables USB, external storage, and clipboard access for production environments. Access occurs only through secure, monitored workstations and VPN connections. Activity logs and AWS CloudTrail alerts notify administrators of any unauthorized access or data transfer attempts, ensuring immediate

Provide your organization's privacy and data handling policies to describe how Amazon data is collected, processed, stored, used, shared and disposed. You may provide this in the form of a public website URL.

Sellwell CMS follows strict privacy and data handling practices. All Amazon data is collected via secure, authenticated API requests over HTTPS. Each request is encrypted before processing, and encrypted data is stored in the database using AES-256 encryption. Data is used solely for

Describe where your organization stores Amazon Information at rest and provide details on any encryption algorithm used.

subnets. All data is encrypted using AES-256 encryption at rest through MongoDB's native encryption and encrypted EBS volumes. Access to the database is restricted to authorized backend services via private connections. No unencrypted data is stored or exposed, ensuring compliance with Amazon's data protection and confidentiality requirements.

Describe how your organization backups or archives Amazon Information and provide details on any encryption algorithm used.

mechanisms and/or AWS snapshots stored in private, secure storage. All backups are encrypted at rest using AES-256 encryption via MongoDB's native encryption and AWS KMS-managed keys. Backups are retained according to data retention policies, access is restricted to authorized personnel, and encrypted backups are securely deleted when no longer needed.

Describe how your organization monitors, detects, and logs malicious activity in your application(s).

detection and security alerts for suspicious behavior, including unusual API requests or failed authentication attempts. Alerts are sent to administrators in real-time, and all logs are retained and reviewed periodically for auditing and incident response.

Summarize the steps taken within your organization's incident response plan to handle database hacks, unauthorized access, and data leaks.

immediate isolation of affected systems, and analysis of logs to assess impact. Malicious activity is removed, vulnerabilities patched, and credentials rotated. Stakeholders are notified if needed. Systems are securely restored and monitored, and post-incident reviews are conducted to improve controls and prevent future breaches.

How do you enforce password management practices throughout the organization as it relates to required length, complexity (upper/lower case, numbers, special character) and expiration period?

case letters, numbers, and special characters. Passwords are stored hashed and salted using secure algorithms (e.g., bcrypt). Expiration policies require periodic password updates, and users are prevented from reusing previous passwords. Multi-factor authentication (MFA) is enabled to further secure accounts.

How is Personally Identifiable Information (PII) protected during testing?

(names, emails, addresses) are obfuscated. Test environments are isolated from production, access is restricted to authorized personnel, and all data in transit and at rest remains encrypted using TLS and AES-256.

What measures are taken to prevent exposure of credentials?

Secrets Manager, never hardcoding them. All sensitive data is encrypted in transit and at rest. Role-based access control restricts access, and multi-factor authentication plus regular rotation enhance security. Logging and monitoring detect unauthorized access attempts, ensuring credentials remain protected.

How do you track remediation progress of findings identified from vulnerability scans and penetration tests?

Sellwell CMS tracks remediation progress through a structured vulnerability management process. Findings from vulnerability scans and penetration tests are logged in a centralized issue tracking system. Each finding is assigned a priority, owner, and remediation deadline.

How do you address code vulnerabilities identified in the development lifecycle and during runtime?

lifecycle. Code is scanned with SAST tools, reviewed for secure practices, and dependencies are checked. DAST and penetration tests identify runtime issues before deployment. In production, continuous monitoring and logging detect suspicious activity, and patches or mitigations are applied promptly to ensure secure operation.

Who is responsible for change management and how is their access granted? Please specify job title.

management. Access is granted based on role-based access control (RBAC), requiring approval from the Technical Lead or CTO. Changes are performed using authenticated accounts with MFA, and all activities are logged. No direct access is given to general developers, ensuring that only authorized personnel can implement or approve changes to production systems.

☐ **I have read and agree to the Amazon Services API Developer Agreement, Acceptable Use Policy, and the Data Protection Policy**

Cancel Register