### 开发者注册流程

1. 目前看来缺少Amazon Logistics 角色，导致无法注册物流商信息，开Case询问
2. 用现在的销售端的开发者试一下能不能走通流程

### 二、开发者注册表单填写说明：

##### Contact Information：

尽量保持和物流账号信息一致

##### Data Access：

选择 Private Developer

##### 开发者文案：

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

A: (这里需要更改为Shipping所需要的信息)

1. Product Listing & Pricing

Provide a convenient product upload and management capabilities for sellers, providing catelog information, common A+ templates, estimated price, etc., recommended keywords, and provide automation price adjustment tools.

2. Inventory and Order Tracking

Inventory tracking and dynamic update, sales statistics and trend analysis, formulate supply and demand plans, provide stockings for reference.

3. Amazon Fulfillment

FBA Fulfill, FBA stockings and logistics tracking, creation of inbound shipments, Inventory Reports, etc.

4. Direct-to-Consumer Shipping

Merchant Fulfillment. Print product labels. Provide logistics trajectory for sellers. Automatically upload order delivery information.

5.Optimal shipping

According to the delivery address, the principle of nearby configuration is carried out, and the distribution warehouse is selected to improve the delivery time.

6. Buyer Solicitation

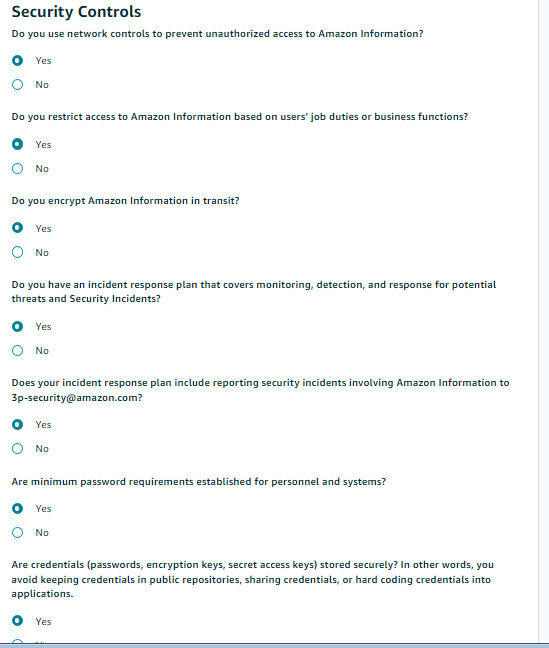
Help sellers to ask for seller feedback and a product review for the choosed asin orders.

7. Buyer Communication

Provide customer service center for the sellers. Help them to manage messaging to and from Amazon buyers.

8. Selling Partner Insights

Provide store performance information, and provide alert about abnormal conditions and suggestions.



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

A: Amazon information is not shared externally.

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

A: No information from non-Amazon MWS sources was found.

PII信息

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

A:Personal identification information is mainly used to generate shipment labels and send Amazon orders directly to buyers.

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

A: We configure the user group access network IP control in the server to allow only specific user group IP to access the database and file server. At the same time, when the user group accesses the database and file server, the user name and password must be entered, otherwise access is prohibited.

Q: 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.

A:

1. Each employee has a unique email and unique UserID, and employees use their email as an account to log in to the system.

2. Our application introduces enterprise sso to control the user's login and access permissions, and also defines the user's role.

3. Different roles have different data permissions.

4. Import information(Such as Client-Secert) would be encrypted and store separated.

Q: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.

A:

1. My application can only be accessed under the company network. The employee’s personal devices do not have the company’s network client.

2.We have purchased professional equipment provide different security strategies, and record the use of employees’ personal devices in detail to ensure data security. Only the system administrator can change the settings for accessing employees' personal devices

3. Every step of the operation of the employees is recorded and archived to prevent data loss.

Q: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.

A:When we collect user information, we strictly abide by Amazon’s privacy data processing policy and must obtain the user’s consent. We will desensitize and anonymize key data and sensitive data, and store it through RSA-2048 encryption. Without the user’s consent, we Resolutely not share or disclose any private data to the outside world.

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

A: Algorithm: AES-256-ECB

Encrypt Developer SerectKey, Sellers' AccessToken, Buyers PII

Store API Encrypted authorization information In Mysql Database.

Store Buyers PII In InfluxDB (TSDB), and automatically expired within 30 days

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

A: We use incremental backup to store Amazon backup information in a private cloud server in our computer room, and use 2048-bit RSA algorithm for encryption. The backup information does not contain PII, and PII is retained for no more than 30 days after the order is delivered.

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

A:

1. Use WAF to intercept external request, determine whether the request is a normal human access. Alert if it is hack attacked

2. Check whether the user login within the common ips, if suspicious login requires email or mobile verification

3. Check whether the user has abnormal behavior, such as deleting a large number of listings, etc.

4. Alert if we got MWS API Error. Such as 'Request is throttled' etc.

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

A:

1. We define several levels of risk or alarm. The highest-level alarms (database hacks) will be notified to the corresponding engineers by phone call. Remind engineers to respond in time.

2. Check whether the data is lost or tampered, we will restore it according to the backup data.

3. Find the reason for the attack and fix it to avoid being attacked again

4. Check whether to cause losses to our customers, we will make corresponding compensation

Q: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?

A:

We set the password in the system to be longer than 18 characters. The password contains uppercase letters, lowercase letters, numbers, and special characters. The password is updated every 60 days. Our account ID and password are our system administrators. Created, employees cannot create their own passwords. We assign account IDs and passwords to employees, and employees must log in with the assigned account IDs and passwords.

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

A: We have a separate test environment and production environment. We require that no PII be kept in the test environment, and PII should be deleted immediately after the test is completed. In a production environment, PII is only used for order delivery and tax invoices, tax remittances, and PII is retained for no more than 30 days after order delivery.

Q:What measures are taken to prevent exposure of credentials?

A: We will not store sensitive information such as credentials in a public code repository. We have established a separate private code library for sensitive information such as credentials, and protected it through encryption. Sensitive information such as credentials must never be hard-coded into the code. Called dynamically in the code.

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

A: The company’s program testing team maintains a test plan. The testing team will perform vulnerability scanning and penetration testing on the application before the program is released, and output vulnerability scanning and penetration testing reports. Based on the test plan, the testing team will fix the vulnerabilities within one working day. Responsible for tracking the progress of the repair until the vulnerability is repaired and written into the test plan.

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

A: The company’s program test team maintains a test plan. The test team will test the code during the development life cycle and during operation every 120 days, and output vulnerability scanning and penetration test reports. The development team will fix vulnerabilities within one working day and test based on the test report. The team is responsible for tracking the progress of the repair until the vulnerability is repaired and written into the test plan.

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

A: The company’s technical director is responsible for change management, the technical director grants the change personnel the minimum change authority through role control, and the change personnel is responsible for completing each change task.