Semrush App Center Technical, Onboarding, Approval, Testing, Security and Branding Requirements for App Partner Product

1. General.

1.1. All App Partner Products must be configured to work properly with the App Center.

1.2. All App Partner Products, and any modifications or updates, must be approved by Semrush in writing before release in the App Center.

1.3. Unless otherwise specified by Semrush (such as in the event of a security issue), or agreed upon between Semrush and App Partner, all onboarding, testing, and approval communications or other notifications between Semrush and App Partner regarding the App Partner Product will be through email or via corporate messenger (Slack or other messenger designated by Semrush) and App Partner shall have ten (10) days to resolve any issues and make any changes required by Semrush.

1.4. If the App Partner Product or any App Partner Materials are causing damage or otherwise interfering with any Semrush Product, Semrush may require an immediate cure or suspend availability of the App Partner Product or App Partner Materials while App Partner is remedying the issue.

1.5. Semrush may reject App Partner Product at any stage of the approval process or in the event that issues are discovered after release of the App Partner Product.

1.6. Onboarding, approval and testing requirements for App Partner Materials shall be as specified by Semrush.

2. Onboarding and Testing Requirements.

2.1. *Onboarding*. The onboarding and approval process must be completed before the App Partner Product may be made available in the App Center. App Partner must:

2.1.1. Notify Semrush that the App Partner Product (or modification) is ready for approval;

2.1.2. Provide Semrush with a demo of the App Partner Product and a description of the App Partner Product functionality;

2.1.3. Complete, fully and accurately, any questionnaires, assessments, or surveys provided by Semrush;

2.1.4. Make any changes requested by Semrush based on the demo, description and questionnaire responses;

2.1.5. Provide Semrush with the App Partner Product landing details, including but not limited to icon URL, caption, App Partner Product description, list of the key features, location, meta title, meta description;

2.1.6. Provide Semrush with the App Partner Product for testing (see 2.2 below), including security tests and make any changes requested by Semrush as the result of such testing; and

2.1.7. Make any changes requested by Semrush as part of the final design review of the App Partner Product.

2.2. *Testing.* The App Partner Product must be tested to validate interoperability with Semrush Products, and to identify vulnerabilities, bugs and other issues that may affect the App Center or Semrush Products. Semrush may provide App Partner, at any time, with a test suite to be performed by App Partner to output log files for Semrush review. Semrush and/or third-party professionals working at the direction of Semrush may review the output log files or test the operation of the App Partner Product to determine whether they indicate sufficient interoperability between the App Partner Products and the Semrush Products, or whether the App Partner Product meets Semrush security requirements. As a result of such tests, Semrush may make suggestions and/or recommendations to modify the App Partner Product to ensure interoperability, resolve issues, or meet security requirements.

3. Technical and Review Requirements.

3.1. Uptime: App Partner Product must maintain an uptime of at least 99%, excluding any downtime that is (a) planned by the App Partner for maintenance purposes with at least seventy two (72) hours' notice to Semrush; (b) caused solely by Semrush; (c) the result of force majeure events beyond the App Partner's reasonable control; or (d) caused solely by a failure of one or more of App Partner' third party vendors, despite App Partner's best efforts to adequately remedy such a failure. App Partner shall notify Semrush immediately in the event of any unplanned downtime.

3.2. Ongoing Review: App Partner Product will be subject to ongoing review, technical and otherwise, by Semrush for as long as it is in the App Center. If the App Partner Product is no longer eligible for the App Center, Semrush will notify the App Partner and will allow the App Partner ten (10) business days to remedy the issue(s), as determined by Semrush in its sole discretion.

3.3. No Extraneous Code: The App Partner Product must not have any code or component that is unrelated or unnecessary to its proclaimed services and functions.

3.4. Tracking: App Partner may track in-app usage via services approved by Semrush provided that any such tracking is both in accordance with the Semrush Terms (as defined in the Semrush App Center Partner Agreement) and App Partner's privacy policy and all applicable laws and regulations. App Partner shall provide Semrush with appropriate IDs in such services and the list of cookies prior to any in-app usage tracking. Any changes to the list of services and the list of cookies shall be provided by App Partner in advance for approval by Semrush. Semrush reserves the right to prohibit such tracking in its sole discretion.

3.5. Miscellaneous: App Partner and App Partner Product also shall comply with the following requirements, which might be changed at the Semrush discretion: Miscellaneous Requirements.

4. **Modifications to the App Partner Product.**

4.1. Semrush shall be informed of any modifications to the App Partner Product (including new releases and updates) in advance, Semrush will advise if the modification shall go through the process listed above (or such abbreviated process as Semrush may specify depending on the nature of the modification), including any modifications that impact security or interoperability.

4.2. If modifications to the App Partner Product adversely affect interoperability between the App Partner Products and the Semrush Products, then Semrush may offer suggestions to App Partner. If App Partner agrees to implement such suggestions, App Partner shall within 30 days after receipt of the suggestions, resubmit the App Partner Product for approval, and, if applicable, include an updated interoperability guide for interoperability testing. If the new submission is approved, Semrush will make the new App Partner Product available in the App Center. Otherwise, Semrush will keep available the App Partner Product version prior to the modifications.

4.3. If any modifications affect the security of the Semrush Products and/or Semrush Content, or the security of any integration with App Partner Product, Semrush will notify the App Partner and, until the changes are made and approved by Semrush, Semrush may suspend availability of the App Partner Product in the App Center.

5. **Audit.**

5.1. App Partner agrees to permit Semrush and/or third-party professionals working in our direction, to review or audit App Partner's records, access logs, third-party audit and examination reports, systems, networks, technologies, facilities (including physical and remote access to data centers and cloud facilities), controls, processes, policies and procedures to ensure compliance with Semrush security requirements. You will obtain all permissions needed for such an audit and will provide reasonable assistance during the audit. Any such audit will be conducted during normal business hours and with reasonable prior written notice. If any audit reveals any noncompliance: (i) you will reimburse us for all reasonable costs and expenses of such review and all re-reviews (if the noncompliance was material) and (ii) you will immediately remedy such noncompliance. Any information obtained by Semrush during such audits or disclosed by you or third-party under this Section is subject to confidentiality obligations set forth in the Semrush Terms.

5.2. For the avoidance of doubt the audit rights set forth in this Section 5 shall be limited to code specific for security or for integration of the App Partner Product features into the Semrush Products. Semrush shall not request or be given access to any server or other codebase except as expressly set forth herein, and Semrush shall not attempt to reverse-engineer App Partner's codebase.

6. **Brand Identity Requirements.**

6.1. App Partner and App Partner Product also shall comply with the Semrush brand identity requirements, which might be changed at the Semrush discretion: Brand Identity Requirements. Certain branding elements are prohibited for use in App Partner Product.

Semrush App Center Security Requirements for App Partner Product

1. **General**

1.1. App Partner must use industry-standard security measures appropriate for App Partner Product and Semrush Security requirements are located here and subject to changes at Semrush discretion: Security Requirements. In addition, App Partner must comply with any applicable security standards, secure coding practices, authentication, data encryption at rest and in transit, or other requirements for App Partner Product in this document or any other Semrush security policies or procedures, including Security Incident Policy. App Partner agrees to remediate all security vulnerabilities identified to you by Semrush within the timeframes specified herein.

1.2. Semrush, or an authorized third party selected by us, may conduct a security review of any App Partner Product or its supporting infrastructure related to your compliance with your obligations under these requirements. Security reviews may include, without limitation: information requests to you, reviews of your documentation, interviews, security testing, technical testing and reviews, event logging, network testing, and vulnerability threat assessments. In addition, Semrush reserves the right to request that you provide the part of code of any App Partner Product that is involved in any Security Incident (as defined in Security Incident Policy), but solely for the purpose as a part of the investigation process due to the Security Incident. You agree to reasonably and promptly cooperate with such requests and with Semrush's review of your App Partner Product and/or your App Partner Product's supporting infrastructure.

Semrush App Center Security Incident Policy

1. **General**:
    1.1. "Security Incident" means any actual or suspected unauthorized access, acquisition, use, disclosure, modification, security vulnerability or compromise of any App Partner Product or Customer Data, or any other issue involving any App Partner Product that materially degrades any Semrush Product or introduces any security vulnerability to any Semrush Product.
    1.2. Upon discovery or notice of any Security Incident, you will promptly notify Semrush via email (security@semrush.com) and any other additional methods as Semrush may specify (such as Slack or other messenger designated by Semrush). Such notice will include information about the Security Incident and how it may affect Semrush Customers and Semrush Products, and shall contain the information set forth in below.
    1.3. We may request other information related to the Security Incident. Without limiting your other obligations, in the event of a Security Incident, you will be solely responsible, at your own expense, for investigation, remediation of the Security Incident.
    1.4. Without limiting any other reserved rights of termination or suspension, Semrush may suspend the availability of the App Partner Product in the App Center.

2. **Security Incident Response**:

    2.1. If you've experienced a Security Incident, you shall take the following steps:
        2.1.1. Make all the necessary notifications:
            2.1.1.1. Promptly (and no later than 24 hours) notify Semrush about the Security Incident and provide the requested information outlined below.
            2.1.1.2. Notify Customers and/or data protection authorities if such notification is mandatory under your privacy policy and/or applicable data protection laws, provided, however, that any notification that mentions Semrush or the App Center or any Semrush Product must be approved in advance by Semrush.
        2.1.2. You may be asked by Semrush to provide further information and assistance related to the Incident, so make sure you have an updated contact for Security Incidents.
        2.1.3. Information that Semrush will need includes answers to the following questions. If you do not have all the information below when a Security Incident is initially discovered, provide all the information you have to Semrush and provide updates when you have more information available.

Question	**Details**
What is the category of Security Incident that has occurred (e.g., vulnerability, malicious attacker, cross tenant data leakage, etc.) and its scope?	Information about the type of incident that has occurred, how long it has been present, and the extent to which Customers may have been impacted.

What type of data was included in the data breach?	If data was breached or leaked, list the types of data included. This can include data other than Customer Data.
Do you have an anticipated / expected timeframe in which you expect the Security Incident will be resolved?	Estimates you might have as to how long it will take for you to resolve the incident and your reasons for the timeframes provided.
What measures have been taken so far, or do you plan to take, to contain the Security Incident?	Describe what action was (or will be) taken to contain the Security Incident.
Has the underlying issue / cause of the incident been identified? If so, please provide details.	Describe the results of any investigations that have been undertaken to identify the underlying issue(s) / root causes of the Security Incident.
What remedial actions have been taken to remove the root cause of the Security Incident and prevent similar incidents occurring in future?	Describe the remedial or corrective actions – both in terms of technical and organisational controls – to prevent similar incidents happening in the future.
What are the contact details for the appropriate person to contact on this issue should Semrush wish to communicate further?	Provide email address and phone number at minimum.

3. Investigate the Security Incident

- Identify the root cause of the incident, for example, by consulting logs, reviewing code, etc.
- Confirm whether any end user data might have been compromised.
- Determine how long the security issue might have been present.
- Determine which users of your app were affected and all information that was or may have been compromised.
- Consider engaging external help such as an incident response partner or security consultant to help with this process if required.
- At the Semrush sole discretion, Semrush also may help you with reviewing evidence, logs and reviewing response plan.

4. Contain the Security Incident

- Contain the Security Incident as rapidly as possible to prevent further impacts to Customers.

- This may require making the decision to temporarily restrict access by Customer to App Partner Product. For example, you (or Semrush) might delist App Partner Product from App Center while remedial action is being implemented.
- Keep in contact with Semrush no less than every 6 hours via email (security@semrush.com) and any other additional methods as Semrush may specify (such as Slack or other messenger designated by Semrush) to provide updates on the progress of remediation efforts and details of specific actions taken.

5. Implement remedial measures

- Take remedial or corrective actions to prevent similar Security Incidents happening in the future.

6. Conduct a post incident review

During the aftermath of the Security Incident you must confirm the Security Incident has indeed been fully resolved, and to identify the reasons for Security Incident to prevent them further, including but not limited by the following:

- Are there any indicators of compromise that are still present?
- Are there any lessons that have been learned from the response to the incident that need to be used to update your organization’s incident response process?
- Have any actions been taken to reduce the chances of a similar future Security Incident?
- Does your logging need to be improved in order to expedite investigation for any future incidents?
- Do your external cyber security advisers / incident response firm agree the incident is resolved?

Once you have conducted a post incident review, Semrush may engage with you further to discuss the findings. You should also submit any details regarding findings to the Semrush security team.