Developer Security and SLA Requirements

(Podium Marketplace and Developer Program)

The following are security and service level requirements for listing an App on the Marketplace. Your App must comply with the requirements listed below. Any capitalized terms not defined herein have the meaning set forth in the Podium Developer Terms (currently available at https://partner-terms.podium.com/#developer-terms).

1. You will allow Podium to conduct system vulnerability scans on the provided systems or endpoints on an on-going basis to ensure maximum security and adherence to these requirements.
2. Your App must not collect Podium Clients' user credentials.
3. To the best of your ability, you must follow security best practices and hardening techniques for all aspects of your business.
4. Your App must authenticate and authorize all requests.
5. Your App must be protected against common web security vulnerabilities.
6. If your App stores its own credentials, then it must only store salted password hashes, not plaintext passwords, as described on the Open Web application Security Project website.
7. Your App must always be served over HTTPS using a valid TLS certificate (version 1.3) with an expiration date of at least 1 year from the App submission date.
8. HSTS must be enabled with a minimum age of at least one year.
9. You must provide a Vulnerability Disclosure Policy (VDP) for security researchers to be able to submit findings regarding your App.
10. All OS, web-server, and app-server security patches must be up to date, and new patches must be applied in a commercially reasonable timeframe after they are made available by the hardware and software vendors.
11. You must provide the IP address(es) from which your App operates and from which Podium API calls are made.
12. You must submit a Security Self-Assessment.
13. Your App must generate secure tokens, including expirations and search indexing protections, where applicable.
14. Your App must not expose network services unnecessarily.
15. Your App must not expose its shared secret. If your secret is inadvertently exposed, then you must rotate the secret immediately. They should never be logged, stored in client-side code and public repositories, or made accessible to end-users.
16. Request only the OAuth scopes needed for the documented use of the App.
17. You must own the domain name that you use for your App, your App's privacy policy, support, and landing page URLs, or get the appropriate permission from the domain name owner.
18. Your App must protect against iFrames using frame-ancestor Content-Security Policy directives (if applicable).

19. Caching is disabled on all SSL pages and all pages that contain sensitive data by using value no-cache and no-store instead of private in the Cache-Control header.
20. Your App web server must be configured to disable the TRACE and other HTTP methods if not being used.
21. You must include a link to a privacy policy in your App listing to communicate how your App uses data, and to help build trust with businesses using Podium.
22. Your App must not provide third-parties with access to a Client’s Podium data, via external API calls or any other means.
23. Your App must not export, save, or store End-User Data for any purpose other than the functional use of your App.
24. If your App is used by organizations based in Europe, or organizations with customers based in Europe, then it's your responsibility to make sure that your App is GDPR compliant.
25. Your App must subscribe to mandatory webhooks so that you can receive any data deletion requests that are issued by organizations. If applicable, your App must subscribe to mandatory GDPR webhooks.
26. If your App handles a significant amount of End-User Data, then it must have a system in place to manage that data properly, including secure storage and the ability to erase data at the user's request as per the data rights of individuals.
27. You will guarantee 99.9% uptime for your App. If your App has downtime that falls short of the 99.9% uptime guarantee for any 30-day period, Podium may revoke your access to the Marketplace and remove or disable your App. This uptime guarantee does not apply to planned maintenance, so long as such maintenance is communicated to the Podium Clients.