BigID Marketplace Developer Guidelines

This document outlines the BigID Developer Guidelines for creating and publishing solutions (applications, integrations, or connectors) on the BigID Application Marketplace. This information is occasionally updated, so be sure to check back and review from time to time. Please review all of the details below and reach out to BigID if you have any questions or concerns with the information below.

Security

Only users granted access to the submission role on the BigID Application Marketplace will be allowed to submit and publish solutions. BigID assigns these roles at the request of the account owner as identified by the Partner/Customer to BigID.

In the event that a user leaves your company or changes roles, it is your responsibility to notify BigID of the change as soon as possible so access rights can be removed. When a new person needs to be added, the account owner will need to notify BigID via email and BigID will provide the correct credentials to the resource for submission and publishing.

At BigID our goal is to create a high level of trust and security in the Application Marketplace among our users. For that reason, the BigID environment is highly curated and each solution submitted will go through a rigorous review process prior to release on the BigID Application Marketplace. Our reviews include the following:

- Three automated code/image reviews
- Manual review of the code submitted
- Manual review of the Marketing material submitted

If the solution fails any of these reviews, it will be sent back to the submitter with comments on what needs to be updated and resubmitted. In the event there are questions, or concerns with the feedback, the submitter has the right to send a note for more details to appreview@bigid.com.

In preparation for the submission, BigID recommend the following guidelines:

- Thoroughly test your solution prior to submission
- Ensure that the solution information you submit accurately reflects the solution
- Make sure that the support and contact information provided on the form is up to date and accurate
- Provide detailed feature/benefit information and quality marketing material
- Ensure that there is no offensive or objectionable content in any of the material

- Ensure that your solution abides by the data security measures outlined in the security section of this document.
- Your solution should implement appropriate security measures to ensure proper handling of user information and prevent its unauthorized use, disclosure, or access by third parties. In your provided setup and support guide, be sure to list all data your application uses and how you are using that data. Processing data that has not been listed will lead to your application failing review.
- Do not treat the Solutions Review Process as a software testing service. We will reject incomplete solutions that cause issues or exhibit obvious technical problems.
- Demos, betas, and trial versions of your app don't belong on the Application Marketplace. If you are looking to have a solution you would like to post as open source, please use bigexchange.bigid.com to post your solution.
- Solutions must be contained within their application bundle. They may not read or write data outside the designated container area, nor may they download, install, or execute code that introduces or changes features or functionality of any installed application
- Solutions that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the core BigID Application will be rejected. Multiple violations will result in the partner/customer having all solutions removed from the program and their access rejected.

Additional Points:

- **Encrypt data at rest and in transit.** Data in transit should use at least TLS 1.2 or greater with a cipher suite currently supported by NIST SP 800-52. Section 3.3.1 and Appendix C provide recommended cipher suites for this purpose. Data at rest should be encrypted with a minimum key length of 256 or greater. If possible, store data within BigID instead of your application.

- **Have an established escalation process.** Have an established process of who will be informed if a vulnerability is found in your application. Be sure that this includes a process for patching your application. Your reporting requirements may vary by jurisdiction, but having a process will not.

- **Establish continuous integration.** Use tools that will automatically check your application (and its dependencies) for security vulnerabilities. When an alert indicates a vulnerability has been found, follow your established patching process to fix it.

- **Make your application accessible.** Your application should follow general accessibility rules (not using color as an indicator of status, filling out ARIA elements, etc). Accessible applications allow users of all abilities to use your application better and support a larger customer base.

- **Use BigID defined authentication mechanisms.** Do not rely on firewalls or "secure networks" to protect your application. All application endpoints should be secured using

BigID provided authentication mechanisms like the UI SDK, BigID API tokens, or a BigID API token derivative such as an access token.

BigID Certified Application

BigID will certify apps which have been submitted with the appropriate criteria and have passed all of the process requirements listed below.

- The submission package must contain the docker image, source code for the app, docker deployment files (docker compose and kubernetes helm chart), and the setup and configuration guide based on the BigID template
- The submission must have a verification code provided by BigID (as part of the Marketplace submission process) included within the application manifest.
- The submission must have passed all of the validation checks, technical and marketing, and be digitally signed using the BigID App Store Certificate Authority.

If the app submitted has all of these items included, BigID will give it an online BigID Certified stamp displayed on the Marketplace, it will be filterable by the customers and placed in our featured section on the Marketplace for a period of time.

If any of the criteria are missing in the above list, the application can still be approved and published to the BigID Marketplace, but it will not contain the BigID Certified Stamp.

General Guidelines

Customers need to know exactly what they are receiving, so please ensure that your application includes clear descriptions, images, documents and links to videos that accurately reflect the solution you have submitted. If you would like more information on the submission process, please review the BigID Solution Submission Guide.

Solutions on the Marketplace are not limited in the number provided by a partner or customer. Unique names, descriptive keywords and clear artifacts will be critical to ensuring that each solution will stand out from the rest. In some cases, review the solutions on the marketplace to ensure that your submission is unique.

Updates or changes to your solution must be clearly called out in the Release notes if you repost a new version of an application. Customers will be instructed to look there for changes should a new version of a solution become available.

In the event you will need a solution removed from the marketplace, you must email marketplace@bigid.com and request removal. Removal requests will only be fulfilled if the request comes from the primary owner or from the solution submission contact.

Solutions that are pure marketing listings on the site will be removed from the Marketplace. In the event that a solution is deemed to be a marketing listing, BigID will notify the partner/customer and they will have the opportunity to remove or correct the listing within 5 business days.

BigID will periodically review all solutions on the marketplace for outdated information, duplicate entries, copies of existing listings, or any other items that are out of compliance with the stated details in this document. In the event that BigID finds an issue, we will notify the partner/customer and they will have 5 business days to correct or remove the solution. In the event that timeline is not met, BigID will remove the listing.