**Instructions: Please provide a yes/no (Y/N) in the yellow shaded area, indicating your ability to meet requirements. If an item is left blank, you will be implying that your company cannot meet the requirement(s), and your proposal may be eliminated from evaluation. This document will be used to evaluate respondents as described in RFP Section 3.2 (Evaluation Criteria), Step 1.**

|  |  |  |
| --- | --- | --- |
| **Item** | **Requirement Description** | **Respondent Answer** |
| **Business Requirements** | | |
| 1 | The payment network system must provide a minimum of 99.9% uptime for 24 x 7 x 365 operations. | Y |
| 2 | The payment network system must be able to process a minimum of 7,800,000 transactions per year for a single enterprise client. The payment network system must be able to process 40,000 transactions per day during peak periods. Further, the service must have the scalability to accommodate significant growth in number of transactions in the coming years. | Y |
| 3 | The payment network system must have the ability to support the following business model: A payment processor hosted checkout that enables all user applications to accept data off the State network. No PCI data flows through the State but white labeled (custom branding) screens are presented to customer. The customer is redirected outside of State's web application to the Contractor's payment gateway and after completed payment the customer is redirected back to State's web application. | Y |
| 4 | The Contractor shall be solely responsible for setting up, in its own name, merchant accounts for each application (POS, Virtual, WEB, etc.) that requires and / or permits the collection of fees from State customers users, whether the application is developed by the Contractor, its Affiliates, or by a third party. | Y |
| 5 | The Contractor shall provide, manage and support Point-of-Sale (POS)/In-Store acceptance (both swipe and key entry), Interactive Voice Response (IVR)/Pay-by-Phone, Website Acceptance (WEB)/Online Entry, Mobile Payment, and other agreed to methods for completing credit card and e-Check transactions with the required functionality, security, and data privacy. | Y |
| 6 | The Contractor shall accept, validate and process the following: Authorizations, Settlements, Full or Partial Refunds. | Y |
| 7 | The Contractor shall accept, validate and process at minimum the following credit card types: Visa, MasterCard, American Express, Discover. | Y |
| 8 | The Contractor shall process all major debit networks for PIN based/less & Signature Debit Cards. | Y |
| 9 | The Contractor shall accept, validate and process: Electronic Checks, including ACH Debits, Guaranteed Electronic Checks. | Y |
| 10 | The Contractor shall process ACH payments to include: ACH Credits, One-time ACH payments over the WEB and IVR, Recurring ACH payments over the WEB and IVR. | Y |
| 11 | The Contractor shall not have minimum or maximum amounts per transaction unless requested by the State Entity. | Y |
| 12 | The Contractor shall direct funds to the State depository designated by the State Treasurer or as outlined in individual Scope of Work documents. | Y |
| 13 | The Contractor shall provide real time notification, where applicable and as requested, of the submitted payment so that the user can see (1) that the payment was successful or (2) a read failure message explaining the issue and (3) hold the pending transaction if it should remain in pending status. | Y |
| 14 | The Contractor shall have the ability to process multi-million dollar payments without multiple payment transmissions, as allowable by the acquiring bank, at which time supporting documentation from the acquirer will be provided by the Contractor. | Y |
| 15 | The payment network system must include a separate fully functional test environment that mirrors the production environment for application development and testing. Further, the test environment should have the same 24 x 7 x 365 availability as production environment. | Y |
| **Implementation Requirements** | | |
| 16 | The Contractor shall successfully transition and implement existing payment processing services by October 20, 2022. | Y |
| 17 | The Contractor shall have the ability to integrate with the States middleware solution (MuleSoft) to provide, or develop, an API for State connectivity to the Contractors payment processing solution. | Y |
| **Security Requirements** | | |
| 18 | The Contractor shall support industry standard security best practices to include the latest versions of: (a) NIST SP 800-53, (b) Open Source Security Testing Methodology (OSSTMM), US Computer Emergency Response Team (CERT) Best Practices (US CERT) (c) NIST SP 800-53A, NIST SP 800-30, NIST SP 800-37, NIST SP 800-115, and others, and (d) CSIS 20 Critical Security Controls. | Y |
| 19 | The Contractor shall provide a FIPS 140-2 compliant system that will encrypt all financial and confidential data transmitted over the Internet. | Y |
| 20 | The Contractor's Payment Processing Solution shall provide a system that is protected by security, using a public certificate authority to ensure that connected clients are on the Contractor's system. | Y |
| 21 | The Contractor shall provide a completed and accepted Report on Compliance that is delivered to and reviewed with the State annually. | N |
| 22 | The Contractor's Payment Processing Solution shall be Payment Card Industry Data Security Standard (PCI DSS) Level 1 compliant based on the most current version of the standards. | Y |
| 23 | The Contractor shall be willing to provide proof of existing and ongoing PCI DSS compliance. | Y |
| 24 | The Contractor shall provide a formal, defense-in-depth security strategy that will be used to provide ongoing security for State resources in the Contractor environment, update the strategy on an ongoing basis, and inform the State in writing within thirty days of strategy updates. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor environment. | Y |
| 25 | The Contractor shall utilize a security testing approach that aligns with the latest version of NIST 800-115, Technical Guide to Information Security Testing and Assessment. | Y |
| 26 | The Contractor shall support file transfers via Secure File Transfer Protocol (SFTP). | Y |
| **Reporting Requirements** | | |
| 27 | The Contractor shall provide the State and Entities same day reporting, monthly reporting, and ad-hoc reporting of individual merchant accounts or the entire State’s supported merchant accounts through its Online System at no cost to the State for the duration of the Contract. These reports will include at a minimum the listing of reports outlined in Attachment J- Scope of Work, Section 1.4.3.1 (3)(ii). | Y |

If Respondent is unable to respond YES to all Minimum Requirements but believes they have an alternative solution, please provide Requirement number, Section number, and alternative solution with an explanation. Alternatives will be reviewed and considered by the State as to whether they satisfy the minimum requirements.

|  |
| --- |
| **Security Requirements, #21: Value Payment Systems submits to an annual security audit by a PCI-Qualified Security Assessor, which creates a Report on Compliance; however, VPS cannot provide the full ROC and will share our PCI-DSS Attestation of Compliance. A service provider that provides its ROC to a merchant may be subjecting the receiving merchant and other customers it serves with unnecessary risk due to the sensitive nature of the information that may be contained in the documentation. VPS will provide the State of Indiana with no less information regarding its PCI-DSS audit compared to other government merchants.** |