**Technical/Information Security Format**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Parameters** | **Comments of the Head of IT/ IT Vendor / IS Auditor** |
| 1. | **Name of Merchant/Biller/ Government Department** |  |
| 2. | **Website Name/URL** |  |
| 3. | **Constitution**  Proprietary/ Partnership Firm/ Pvt Ltd/ Public Ltd / Co-op Society/ Trust/ Individual / Corporation / Educational Institution / Religious Organisation / Registered Charity / Government Agency) |  |
| 4. | **Head of Technology**  Name:  Email:  Tel No: |  |
| 5. | **Application IP address** (IP from which the connection request will be made to SBIePay) (Both Server IP and Public Static IP for testing purposes are to be provided) |  |
| 6. | **Details of hosting service provider for the website** |  |
| 7. | **SSL certificate details**  (Certification type, validity and authority) |  |
| 8. | **Website Technology**  (Java,.Net, PHP, COM/DCOM, HTML5, Python, Others)  **Shopping Cart Details**  (Cubecart, Jhoomla, Magento, OSCommerce, WHMCS, XCart, ZenCart, Others) |  |
|
|
|
| 9. | **Operating System hosting the Website** |  |
| 10. | **Application Server details** (JRUN, TOMCAT, JBOSS, WEBSPHERE, WEBLOGIC, Others) |  |
| 11. | **Web Server details** (Apache, IIS, Others) |  |
| 12. | **Do you have internal security guidelines/ document / policy ?** (Yes / No), (Provide copy of the same) |  |
| 13. | **Whether the database and application servers are behind firewall?** |  |
| 14. | **Whether security patches are reviewed and updated regularly?** (Yes / No) |  |
| 15. | **Whether logs are maintained for all transactions to help establish a clear audit trail and assist in dispute resolution?** (Yes / No), (Provide evidence) |  |
| 16. | **Whether you have an in-house IT team or third party service** **provider**. Name of the service provider with contact details |  |
| 17. | **Do you store Card Number / Cardholder Name / Expiry Date?** (Yes / No) |  |
| 17. a | **Is website PCI DSS certified?** (Yes/ No)  (This is mandatory for websites who want to capture card data on their system). If Yes, then provide 17 a-e |  |
| 17. b | **Do you store Sensitive Authentication** Data (Full Track Data / CVV / VBV Secure Code / Master Secure / PIN/PIN Block) ? (Yes / No) |  |
| 17. c | **Do you store internet banking username and passwords or HPIN**? (Yes / No) |  |
| 18. | **Is Vulnerability Assessments (VA) done for the servers?** (Yes / No). (Provide evidence) |  |
| 19. | **Is Penetration Testing and ASV Scans conducted for all servers, applications and network components?** (Yes / No). If Yes, please provide details. |  |
| The information given above is correct to best of my knowledge and the information given can be used for onboarding purpose. I take complete responsibility of the same.  **Signature & Seal: Designation:**  **Name: Date:** | | |