



Brand and Communications

13 January, 2022

.....
.....
.....

Sub: Request For Quotation (RFQ) to re-construct Prime Bank website.

Technical Specification:

Bidder Name:

SL	Description	Agency's Feedback				Comments
		Fully Complied	Need Customization	Workaround Available	Cannot Customize	
1	Audit Trail & details User Activity Report with Timestamp, Date, IP address, Mac Address etc.					
2	Password Guideline a. Passwords for user-level shall be at least eight (8) characters long, whereas for admin-level passwords shall be at least twelve (12) characters long b. Passwords must contain both upper and lower case characters (i.e. a-z, A-Z); c. Passwords must contain digits and/or special characters/punctuation (e.g. 0-9, !~@#\$\$%^&*()_+=-[]}”";;<.>/?\ ,); d. Same Password cannot Reuse for next three times e. Password should be changed on first time login f. System should have capable to send password through email/SMS etc. g. Password cannot be reset within 1 day, System should have the capacity.					
3	User Management (Role Based access control)					

4	Disable the multiple session options for the site.					
5	Session time out period should be set					
6	SQL Injection prevention					
7	Password should not be hard coded in any application					
8	Application should support inputter-authorizer concept as where applicable.					
9	Authentication should be performed for each privileged request					
10	Authentication must not be based on the knowledge of a secret URL					
11	Authentication failures must always result in the same log message					
12	Default, test or temporary user accounts / ID should not exist					
13	Password brute forcing must be prevented					
14	Username enumeration must be prevented					
15	A denial of service using automatically locked accounts must be prevented					
16	Ability to perform user profile reporting easily, using flexible reporting mechanism.					
17	Session-ids must be generated with sufficient entropy					
18	User generated session-ids must be rejected					
19	Session-cookies must be transmitted via HTTPS					
20	The secure flag must be set on the session cookies					
21	The http only flag must be set on the session cookies					
22	Sessions must be revoked if the session-id is not received via HTTPS					
23	Data mutation must be performed using POST requests					
24	A session-bound token must be validated for each POST request					

25	A conservative size limit must be enforced on uploaded files					
26	Application must be able to protect itself from various application vulnerability issues.					
27	Application must be able to protect itself from Cross Site Scripting Attack					
28	Click jacking should be handled					
29	CSRF should be handled.					
30	Denial of Service Prevention should be handled					
31	System should have file sanitization mechanism for handing file upload features					
32	Source Code should be Hardcoded					
33	XSRF - Using user's logged in session to manipulate					
34	Stored data, logic programming problems, displayed contents that reveals sensitive information etc. must be protected.					
35	Serialization of untrusted data, codes and updates pulled from remote source must be handled securely to ensure data integrity.					
36	Session Hijack - Compromise user's session by editing and injecting session cookie					
37	SSRF: User-submitted URLs fetched from remote sources must be validated.					
38	Thin client deployment over internet must be secured by 256-bit SSL and PKI Application must be flexible on adding new feature in future without alerting any.					
39	Ability to encrypt passwords and other sensitive data based on industry-standard encryption mechanisms.					
40	Ability to configure the system using parameter-or table-driven approach. This includes data structures, screens, functions, key fields and reports.					

41	Ability to linearly scale based on reasonable growth patterns by adding incremental computing resources. Also to support clustering at each layer i.e.. Web server, Application Server and Database for Fault Tolerance & Load Balancing. The system would be developed to support clusters environments on N servers.					
42	The application should be parameterized to facilitate initial system set-up and future maintained activates.					
43	Application must allow user-defined archival period and provides the necessary archival tools.					
44	Details Diagram of Application platform / architecture?					
45	What is the Application Framework? Latest Framework will be preferable.					
46	Supported Browser (should be independent)					
47	Browser Version Compatibility issue (if any)					
48	How access control is managed, whether it can be customized?					
49	Any kind of System notification by Email, SMS, Dashboard to System Administrator? System should be capable to have Email, SMS Notification to All kind of Users; In addition System Should have a Comprehensive Dashboard also.					
50	End Point Security related suggestion to implement in Database, Application or Web Server					
51	Should Application server and Database Server will reside in the same server or in different server?					

52	How PBL will approach if any BUG is detected during Post Live operation? How the Change request will be attended by vendor?					
53	If power gets down at client end then how the data consistency will be maintained?					
54	How memory overflow will be handled?					
55	Application should be Single Page Application (SPA)					
56	Application should be responsive from any device (desktop/laptop/mobile/tablet/or any other devices).					
57	Application should be SEO friendly.					
58	Is this application support container based platform /Micro service? (Docker/Kubernetes)					
59	How you will provide required Patches for new change request?					
60	What will be the Deployment Model (On-premise or cloud)? If cloud then where the data will be stored.					
61	What is the Brand, Model, Storage of the server you suggested?					
62	Please provide Detail system architecture. Mentioned the tier of your architecture.					
63	Is this system support virtualization- VMWare?					
64	Provide detail hardware sizing (application, database, web server or any other server mentioned in architecture) considering below: 1. In DC: live, backup and testing/UAT system environment 2. In DRS: live system environment, backup 3. High Availability (HA) of application, database, web server or any other else mentioned in architecture.					
65	Mentioned Supported OS? (Red Hat, Windows or any other else)					

66	Mentioned the Web service used (Apace/Tomcat/IIS/or any other else)					
67	What type of load balancer will be used?					
68	Mentioned supported Database Platforms?					
69	The Application should apply checks to ensure that: <ul style="list-style-type: none"> - no part of the database has been lost - data within the system is consistent - Information has been written to the database consistently. 					
70	Please mention your licensing model (user basis/perpetual/or any other model).					