केनरा बैंक Canara Bank

Corrigendum-1 to GeM Bid ref. no. GEM/2023/B/4044781 dated 05/10/2023 for Selection of Service Provider for Supply, Installation, Implementation and Maintenance of Enterprise Mobility Management Solution for a period of Three (3) Years in Canara Bank

It is decided to amend the following in respect of the above GeM bid:

Sl. No.	Section/Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
a.	Annexure-16 Bill of Material		Existing Annexure-16 Bill of Material	**Amended Annexure-16 Bill of Material**
b.	Annexure-10 Technical & Functional requirement		Existing Annexure-10 Technical & Functional requirement	**Amended Annexure-10 Technical & Functional requirement**
c.	Annexure-7 List of Major Customers of the Bidder in Last 3 Years and References		Annexure-7 List of Major Customers of the Bidder in Last 3 Years and References	Annexure-7 List of Major Customers of the **Bidder/OEM** in Last 3 Years and References
d.	Annexure-2 Pre-Qualification Criteria		Existing Annexure-2 Pre-Qualification Criteria	**Amended Annexure-2 Pre-Qualification Criteria**
e.	Annexure-9 Scope of Work	1.General	f. As the late sign-off of any solution may impact the Warranty / AMC timelines under back-to back agreements of bidder with OEM, they are advised to take care of the same in their agreements with OEMS. The Bank will not consider any request for adjustments in such cases and will seek full five-year active life of each solution with full OEM support & services	f.As the late sign-off of any solution may impact the Warranty / AMC timelines under back-to back agreements of bidder with OEM, they are advised to take care of the same in their agreements with OEMS. The Bank will not consider any request for adjustments in such cases and will seek full **three-year** active life of each solution with full OEM support & services
f.	Annexure-9, Scope of Work	7. Compliance	a. The bidder's solution must comply with guidelines of RBI/ MeitY/PCI or any other guidelines of GOI or any regulatory	The bidder's solution must comply with guidelines of RBI/ MeitY/PCI or any other guidelines of GOI or any regulatory

			authorities in respect of Breach and Attack Simulation Tool issued from time to time.	authorities in respect of **Enterprise Mobility Management Solution** issued from time to time.
g.	Annexure-9 Scope of Work	7. Compliance	b. Data captured in the solution should not be stored outside the Bank's Network.	**This Clause stands deleted.**
h.	SECTION D - BID PROCESS	5.2 Part B- Commercial Bid	The Commercial Bid (Indicative) of only those bidders who are qualified in Part-B Technical Proposal will be opened online. The qualified bidders as per the GeM terms and conditions will be eligible to participate in the Online Reverse Auction	The Commercial Bid of only those bidders who are qualified in **Part-A Technical Proposal** will be opened online.
i.	SECTION F - OWNERSHIP & AWARDING OF CONTRACT	10. Security Deposit/ Performance Bank Guarantee	If the Security Deposit /Performance Guarantee is not submitted within the time stipulated above, penalty at 0.50% for each completed calendar week of delay or part thereof on the total value of the order will be deducted from the delivery payment or from any other payments for the delay in submission of Bank Guarantee. The total penalty under this clause shall be restricted to 1.5% of the total order value	If the Security Deposit /Performance Guarantee is not submitted within the time stipulated above, penalty at 0.50% for each completed calendar week of delay or part thereof on the total value of the order will be deducted from the delivery payment or from any other payments for the delay in submission of Bank Guarantee. The total penalty under this clause shall be restricted to 5 % of the total order value

All the other instructions and terms & conditions of the above GeM Bid shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject GeM bid.

Date: 21/10/2023
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical IT Wing, H.O., Bengaluru - 560 001

केनरा बैंक Canara Bank

Annexure-16
Bill of Material

SUB: RFP for Selection of service provider for Supply, Installation, Implementation and Maintenance of Enterprise Mobility Management Solution for a period of three (3) years in Canara Bank

Ref: GEM/2023/B/4044781 dated 05/10/2023.

Notes

1. These details should be on the letterhead of Bidder and each & every page should be signed by an Authorized Signatory with Name and Seal of the Company.
2. The base location for the project execution would be Bangalore.
3. The consultant will have to work as per the timings of the Bank.
4. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
5. Do not change the structure of the format nor add any extra items.
6. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

Table -A

Price details of Enterprise Licenses for the Enterprise Mobility Management Solution

[Amount in Indian Rupees]

Sl. No.	Item Details	Unit Price (Excl. of Taxes)	No. of years	Qty.	Total cost (Excl. of Taxes)	Tax for Column c		Total Cost (Incl. of Tax)
						% of Tax	Tax amt.	
		a	b	c	d=a*b*c	e	f	g=d+f
1.	Enterprise subscription based Licenses for the Enterprise Mobility Management Solution with comprehensive Technical Support.		3	30,000				
2.	Additional Licenses		3	#20,000				
	Total Cost for Enterprise Licenses for the Enterprise Mobility Management Solution (Sum of column of rows 1 and 2)							

For the 20,000 nos. of additional licenses, Bank at its discretion may procure the within the contract period of 3 years at the rates mentioned above.

Table -B

Price details for Hardware/Software for Enterprise Mobility Management Solution in Canara Bank

[Amount in Indian Rupees]

Sl. No.	Requirement Details	Unit Price with Three years Comprehensive onsite warranty and support (Excl. of Tax) for EMM Solution	Quantity	Total Cost with Three years Comprehensive onsite warranty and support (Excl. of Tax) for EMM Solution	Tax for Column C		Total Cost with Three years Comprehensive onsite warranty and support (Incl. of tax) for EMM Solution
					%tax	Tax Amt.	
		a	b	c=a*b	d	e	f=c+e
1.	Hardware/ Appliance including OS & other software for EMM Solution for DC (specify the list of items serially)						
2.	Hardware/ Appliance including OS & other software for EMM Solution for DR (specify the list of items serially)						
3.	Any other Software / Licenses						
4.	Total Cost for Hardware/Software including licenses etc. for Enterprise Mobility Management Solution (Sum of column of rows 1,2 and 3)						

Bidder has to provide the adequate quantity of items in Column-b of Table-B as required to cover the entire Scope of Work and Technical Requirements as mentioned in the document.

Bidder has to provide the details of all items quoted such as Hardware, Software, Operating System, Licenses, etc. along with its specification details in the as per Annexure-10 (A).

Table -C

Cost of the one-time implementation cost for the Enterprise Mobility Management Solution

[Amount in Indian Rupees]

Sl. No.	Item Details	Unit Price details (Excl. of Taxes)	Qty.	Total cost (Excl. of Taxes)	Tax for Column c		Total Cost (Incl. of Tax)
					% of Tax	Tax amt.	
		a	b	c=a*b	d	e	f=c+e
1.	One Time Implementation Cost, Configuration, Integration, UAT & Go Live as per Scope of Work and Technical Requirements of the RFP						
Total Cost of One-time implementation							

Table-D

Charges for Onsite Resources after Go-Live

[Amount in Indian Rupees]

Sl. No.	Description	Charges for one resource Per Month [Excl. of Taxes]	No. of Months	No. of Resources	Total Charges for resources [Excl. of Taxes]	Tax for Column d		Total Charges for resources [Incl. of Taxes]
						% of Tax	Tax Value	
		a	b	c	d=a*b*c	e	f	g=d=f
1.	L1 Support		36	3*				
2.	L2 Support		36	1*				
	Total Cost for Onsite Resources for EMM Solution							

Note: *The count mentioned in Table-D is indicative only. Bank at its discretion can avail onsite resources based on the requirement. Bank can at its discretion decide the number of resources in case of Onsite support. The charges quoted above shall be fixed for the entire contract period.

Table E - Total Cost of Ownership Contract Period of 3 years

[Amount in Indian Rupees]

Sl. No.	Details	Total Cost of Ownership [inclusive of taxes]
1.	Cost of Enterprise Licenses (subscriptions) as per Table-A	
2.	Cost of the Hardware/Software as per Table -B	
3.	One-time implementation cost as per Table-C	
4.	Charges for Onsite Resources after Go-Live as per Table-D	
5.	Total Cost of Ownership Contract Period [Sum of row 1 to 4 of the Table-E]	

Undertaking

i. Bill of material is submitted on the letter head and is signed by an Authorized Signatory with Name and Seal of the Company.

ii. We confirm that we have gone through RFP clauses, subsequent amendments and replies to pre-bid queries (if any) and abide by the same.

iii. We have not changed the structure of the format nor added any extra items. We note that any such alternation will lead to rejection of Bid.

iv. We agree that no counter condition/assumption in response to commercial bid will be accepted by the Bank. Bank has a right to reject such bid.

v. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.

vi. We confirm that all out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this tender and subsequent agreement is included in the amounts quoted and we shall not entitle to charge any additional costs on account of any items or services or by way any out of pocket expenses, including travel, boarding and lodging.

vii. We confirm that there shall be no escalation in the agreed prices.

Date

Signature with seal
Name:
Designation:

Annexure-2
Pre-Qualification Criteria

[On Firm's / Company's letter head]

SUB: RFP for Selection of service provider for Supply, Installation, Implementation and Maintenance of Enterprise Mobility Management Solution for a period of three (3) years in Canara Bank

Ref: GEM/2023/B/4044781 dated 05/10/2023.

We have carefully gone through the contents of the above referred RFP along with replies to prebid queries & amendment, if any and furnish the following information relating to Qualification Criteria.

Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria	Bidders Response
1.	Signing of Pre-Contract Integrity Pact	The Bidder should submit signed Pre-Contract Integrity Pact on Non-Judicial Stamp Paper of Rs.200/- or as per respective state Stamp Act whichever is higher as per Appendix-F.	
2.	The Bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.	Certificate of local content to be submitted as per Annexure-5 as applicable.	
3.	The Bidder should be a partnership firm registered under LLP Act, 2008/ Indian Partnership Act, 1932 or Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 and should have been in operation for a period of at least three years as on RFP date.	Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company (OR) Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.	
4.	Bidder shall be the Original Equipment Manufacturer (OEM)/ Original Software Owner (OSO)/ Original Software Developer (OSD) of Solution. (OR) An authorized dealer/distributor of the proposed Solution	If the applicant is OEM, an Undertaking Letter has to submit in this effect. (OR) If the bidder is an authorised dealer/ distributor, an authorisation letter from their OEM/ OSO/ OSD to deal/market their product in India and it should be valid for entire contract period from the date of submission of the bid.	

5.	The **Bidder/OEM** should have successfully implemented Enterprise Mobility Management for a minimum of 5,000 users/devices in at least one Scheduled Commercial Bank /BFSI/ PSU/ Government Organization during last three financial years(2020-21, 2021-22 & 2022-2023) in India.	The **bidder/OEM** should submit Satisfactory performance certificate from clients/ copies of purchase order/work order/ reference letter from the clients to this effect.	
6.	The Bidder should have and **average annual turnover** of Rs.50.00 Crores in the last three financial years (**i.e., 2019-20, 2020-21 & 2021-22**). This must be the individual company turnover and not of any group of companies.	Bidder has to submit audited Balance Sheet copies for last **3 Years i.e. 2019-20, 2020-21 & 2021-22** along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number.	
7.	The Bidder should have positive Net Worth as on 31/03/2022 and also should have not eroded by more than 30% in the last three financial years ending on 31/03/2023.	The Bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.	
8.	The Bidder should agree and comply with the Bank's security policy and regulators i.e. Govt. of India / RBI / CERT-IN/NPCI/ DeitY/MeitY/SEBI/AMFI etc. guidelines; industry guidelines as well as complying with other country's regulatory guidelines wherever applicable	Self-declaration cum undertaking to be submitted	
9.	Bidders should not be under debarment/blacklist period for breach of contract/ fraud/ corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking / State or Central Government or their agencies/ departments on the date of submission of bid for this RFP.	The Bidder should submit self-declaration on the Company's letter head to this effect.	
10.	Any Bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the Bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means:	A declaration stating "We have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be	

	a. An entity incorporated, established or registered in such a country; or b. A subsidiary of an entity incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established or registered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.	submitted in Company's letter head. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence / certificates confirming compliance to Qualification Criteria should be part of the RFP.

Date:
Place:

Signature with seal
Name:
Designation:

Annexure-10
Technical & Functional requirement

SUB: RFP for Selection of service provider for Supply, Installation, Implementation and Maintenance of Enterprise Mobility Management Solution for a period of three (3) years in Canara Bank

Ref: GEM/2023/B/4044781 dated 05/10/2023

Bank intends to select bidder with the primary objective of the following:

Vendor is requested to furnish the appropriate response to the particulars asked by giving the compliance level as explained below. Explanations/suggestions by the vendor may be given in the Remarks column. If more explanation of a point is needed, documents can be attached to the Remarks Column in any section.

Compliance	Description
Yes	The vendor has capability of delivering in line with mentioned parameters.
No	The vendor doesn't have capability of delivering in line with mentioned parameters.

The specifications of proposed Enterprise Mobility Management are detailed below. These specifications are only indicative but not exhaustive.

Sl. No.	Technical Specifications	Mandatory(M) / Optional(O)	Bidders Response (Yes/No)	Remarks
Mobile Device Management				
1.	EMM should simplify mobility management, integrating mobile device management (MDM), mobile application management (MAM), Mobile Browser Management (MBM), Mobile Content Management (MCM), Mobile Email Management (MEM), Mobile Identity Management (MIM) into one comprehensive, single console solution.	M		
2.	EMM should provide flexible, comprehensive tools to secure data, deliver apps and content, MDM should give users what they need to be productive without compromising security or the user experience	M		
3.	EMM should centrally manage app protection and compliance policies across all apps.	M		
4.	Identify and track mobile device licenses	M		
5.	Disable some/all pre-installed applications that come with a commercial device	M		
6.	Restrict or manage the "side loading" of applications to prevent unapproved installation of applications by removable media and / or USB connection.	M		

7.	Place prohibited applications installed on device in quarantine	M		
8.	Recognize multiple devices per user and support tenant wise separate permission for number of devices.	M		
9.	Enforce device authentication before device use	M		
10.	Support multi-tenant architecture, multi domain with customized branding	M		
11.	Provide app access through the creation of secure tunnel	M		
Controls and Policies: EMM should implement granular control with comprehensive per app policies including:				
	User authentication and re-authentication requirements:			
1.	In addition to password/PIN based authentication the solution should support integration with 2- Factor systems **(Biometric or Mobile OTP)**	M		
2.	Local data storage control	M		
3.	Enabling document sharing, copy/paste, data loss policies	M		
4.	Remote wipe individual applications, without affecting personal email and apps	M		
5.	Single sign-on authentication across native apps, with offline pin/access/authentication]	M		
6.	Supports integration with Directory Services (Active Directory, LDAP) to fetch existing directory services structure into the MDM solution such that changes in the AD/LDAP are synchronized with the solution in a secured manner.	M		
7.	Enable copy/paste, sharing , editing and opening of data and attachments only into authorized apps	M		
8.	**Control attachment size limits**	O		
9.	Save attachments to a secure folder within the app with no access to personal apps	M		
10.	Manage password policies, including length, complexity, history, expiration, and lockout.	M		
11.	**Require AES-256 encryption for all data including all types of removable storage devices and also data on SD Card**	M		
12.	Supports S/MIME signing and encryption	M		
13.	Sync and share apps across desktop, mobile and web.	M		

14.	Provide access to content repositories, such as SharePoint, Windows File Share, Box, Google Drive, etc.	M		
15.	Self-service distribution of apps to employees and other authorized users	M		
16.	Custom, branded enterprise app store	O		
17.	Convenient, single location for users to install the apps	M		
18.	Control which apps users are authorized to view and install with role-based policies	M		
19.	Allow users to rate and review apps	O		
20.	Reporting on app downloads	M		
Device Management for Mobile Devices				
1.	EMM solution should have centralized system for device management for the complex and heterogeneous mobile device landscape (iOS, Android).	M		
2.	Mobile Device Management solution should have mobile email and application rollouts, safeguard mobile data and devices, and gain comprehensive visibility and control of the mobile environment, regardless of platform, device type or service provider.	M		
3.	Mobile Device Management solution should have user-friendly processes to enroll, deploy, and configure all mobile devices, applications, and content for the enterprise. Solution should support Apple Device Enrollment Protocol (DEP) and Zero Touch for android.	M		
4.	The solution should send enrolment requests over-the-air using message services, email or a custom URL, QR	M		
5.	The solution should authenticate against Active Directory / LDAP, one time pass codes or Security Assertion Markup Language (SAML) based authentication.	M		
6.	Mobile Device Management solution should allow mobile administrators to enable policy controls from passwords and application restrictions and remote actions like device lock or wipe. Security options include: • Policy options (e.g., passwords, remote wipe, app restrictions) can be targeted to specific users/ groups and organization/corporate vs. personal devices.	M		

	• Enforcement of mobile email access policies using email gateway or certificates.			
7.	Mobile Device Management solution should provide prevention of enterprise data loss and elimination of privacy concerns by separating organization/corporate and personal data. It should remove only organization/corporate data upon employee departure, without touching personal data. Identify only organization/corporate email, apps, docs, and any other content.	M		
8.	Mobile Device Management solution should provide cross-platform device management, with enterprise directory integration, role- based access control and content delivery.	M		
9.	Mobile Device Management solution should support with role-based access control. Organizations should be able to leverage the native reporting capabilities built into the system using predefined and customizable reports or leverage the product 's APIs for reporting via third party or internal reporting systems.	M		
10.	**Mobile Device Management solution must have a unified device management across mobile operating systems, including iOS, MAC, Android and Windows through a central console. (Linux OS support may be considered as good to have)**	M		
11.	The solution should integrate with Android for work and Apple DEP	M		
12.	Mobile Device Management solution should provide end-user friendly apps delivery for mobile devices of web apps, organization/corporate apps and third-party apps. It should support both push delivery of organization/corporate required apps and on-demand delivery of end user selected optional apps.	M		
13.	Mobile Device Management solution should report exact details of enterprise mobile assets at all times by leveraging built-in dashboards, reports, and alerts. Provides user, device, app, and profile details through detail views and customizable reports. Also, the Compliance Violation should be made available in the Dashboard with automated alert triggered to Admin / Users.	M		

14.	Mobile Application Management solution should allow organizations to enable mobile workforce productivity by managing the lifecycle of securing, distributing, and retiring apps. OEM should offer their own business productivity apps and avoid relying on Third-Party business productivity apps.	M		
15.	From one central console, Mobile Application Management solution should easily manage internally developed apps, third party apps, native apps or web apps across personally-owned and corporate managed devices. To safeguard apps and data, IT can apply granular application-level policies related to user authentication, data loss prevention and more.	M		
16.	Mobile Application Management solution must manage apps without managing devices by using a container: Application Management should work with or without mobile device management (MDM) to protect apps and data, not just the device by leveraging Mobile Application Management (MAM) approach.	M		
17.	Mobile Application Management solution should expand mobility: Application Management separates personal and corporate apps, giving organizations more flexibility to enable mobility in BYOD environments and the extended enterprise, without infringing on user privacy.	M		
18.	Mobile Application Management solution should add security by wrapping app to apply a layer of security and policy management, with/without a SDK or source code changes.	M		
19.	Mobile Application Management solution should have Corporate E-mail • secure app that brings organization/corporate email, calendar, contacts, notes, and tasks to the users. • Email data at rest on the device must be protected with FIPS-certified encryption that is independent of the device to help secure organization/corporate data in the event the device passcode is compromised.	M		

20.	Mobile Application Management solution should allow IT administrators to configure security policies such as preventing copy/paste of content or limiting the apps in which email attachments can be opened.	M		
21.	E-Mail should support a wide variety of mail servers, such as Microsoft Exchange, Office 365, Zimbra, using Microsoft Exchange ActiveSync.	M		
22.	Mobile Application Management solution should have work web - secure Web browser to provide safe access to internal Web-based applications and content.	M		
23.	Mobile Application Management solution should provide application management that enables self-service distribution of apps to employees and other authorized users, such as contractors or partners with Corporate App Store.	O		
24.	Mobile Application Management solution should provide SDK to enable in-house applications to be added in the container.	O		
25.	Support for implementation of full kiosk mode for selected set corporate owned devices with different make and models.	M		
26.	In Kiosk mode restrict device to run approved applications.	M		
27.	Kiosk mode must have the ability to restrict browser to a single/authorized web application and support whitelisting / blacklisting sites for browsers.	M		
28.	The solution should prompt users to accept a custom Terms of Use Agreement before gaining access to corporate resources on the device.	M		
29.	The solution should create and distribute customized acceptable usage policy.	M		
30.	Users should get notification in case of any change/modification in the policy.	M		
31.	The solution should support fully automated enrolment and activation process with Minimal User Intervention should provide individual or bulk device enrolments.	M		
32.	Approve or deny new mobile devices on the network in workflow based/automated process.	M		
33.	Enable device sharing and kiosk mode features and support and manage shared devices where a single device is shared among multiple users with granular	M		

	security policies and configurations applied to each user independently of any other users or device-wide policies.			
34.	Use bring-your-own-device (BYOD) privacy settings to block collection of personally identifiable information.	M		
35.	Configure device or email wipe when maximum number of failed attempts is exceeded	M		
Enterprise Mobility Management				
Platform Architecture				
1.	Supports Platform - Android, iOS etc. and higher versions, Windows and MAC (Linux OS support may be considered as good to have)	M		
2.	Support for RESTful APIs for extensibility / workflows	M		
3.	Secure tiered-architecture (database server securely on internal network and not in DMZ)	M		
4.	Grouping of devices and users based on business units, organization groups, geographic locations, device ownership, etc.	M		
5.	Monitor device location for providing contextual authentication	M		
Device Management				
1.	Detect and resist jail-breaking and rooting of device	M		
2.	Can apply policies by device type or OS	M		
3.	Can disable/enable the camera and usage of SD Card.	M		
4.	Determines device compliance based on the OS version	M		
5.	Can configure the device to lock/wipe if the maximum number of failed login attempts is exceeded	M		
6.	Has an automatic policy control that deletes all enterprise policies, profiles, apps and data if the management agent is removed	M		
7.	Remote troubleshooting of enrolled devices and administration.	M		
8.	Mobile asset and GPS tracking lock, perform detection and blocking of SIM change and wipe for lost or stolen devices or personal policies that span across devices.	O		
9.	View detailed hardware and software inventory reports	M		

10.	View application and network performance and data usage with proactive alerting when approaching user thresholds.	M		
11.	Ability to be a trusted certificate authority for establishing secure and trusted connection between mobile devices and enterprise systems by enabling secure communication, authentication and data protection within EMM Solution.	M		
12.	Provide Wi-Fi control-blacklist/whitelist selective Wi-Fi networks and detect and prevent manual override by user.	M		
13.	Monitor device status such as battery life, memory usage and CPU.	M		
14.	All MDM features have to be compatible with all mobile / tablet device make/vendors like Apple, Samsung, Motorola, Acer, Nokia , Nothing, LG, Xiaomi, Oppo, OnePlus, Asus, Vivo etc.	M		
15.	Set up screen lock and enforce password protection as per Bank's policy.	M		
16.	The solution should send alerts on encountering following scenarios • Device has not connected in a period of time. • Device has outdated policies. • Device does not have encrypted data protection • Device does not meet minimum OS version • Device has an installed application that is on disallowed applications list. • Device has an installed application that is not on allowed applications list. • Device does not have an application that is on the required applications list. • Device has uninstalled a previously installed required application	M		
17	Solution must support Geo-Fencing of the enrolled devices	M		
Compliance				
1.	Fully configurable notification system (notify select admins or end users based on select events defined)	M		
2.	The solution should have comprehensive predefined security configuration assessment checks (settings) for different supported platforms as per industry standards such as ISO27001, PCI-DSS, and OWASP etc.	M		

Reports and Logging				
1.	Pre-configured policy reports (Compliance, asset management, applications, email, content, certificates, etc.)	M		
2.	Solution should provide dashboard to provide quick view into real-time deployment data from the admin console and gain a graphical summary of operations and compliance. The dashboard should also provide a comprehensive list of enrolled device and drill down into specific device and user details.	M		
3.	Centralized event log to capture all device and administrative events (logins, policy changes, application updates, configuration updates, etc.), view in the console and export reports	M		
4	The Solution should have the capability to integrate with the SIEM solution for logging and monitoring.	M		
Email Management				
1.	Support email, calendar, and contacts in a containerized environment	M		
2.	Prevent unmanaged / compromised / non-compliant devices from email access	M		
3.	Two factor email authentication	M		
4.	Whitelist applications for opening attachment	M		
5.	Encrypt email attachments (AES 256 encryption)	M		
6.	Rendering E-mail attachments within the containerized E-mail Client.	M		
7.	Disable access to all email attachments upon jailbreak/root detection (without internet connectivity)	M		
8	The Solution must have the ability to restrict the public access of Email Solution of the Bank and allow the same only on the managed / enrolled devices. There should not be any licensing dependency from the Email Solution provider to achieve the use case.	M		
9	The Solution should support browser based as well as Client Based like Outlook etc. on various OS platform such as Android, iOS, MAC, Windows etc.	M		
10	**The Solution should have the capability to frame custom policies for MEM as per the requirement of the Bank.**	M		
11	**The Solution should have the capability to exclude specific users (as decided by the Bank) for accessing corporate emails**	M		

	(conditional access) without EMM Solution. Further, the solution should have the capability to exclude conditional access of emails from endpoints which are in corporate network.			
Other Features:				
1	The Solution should have capability to integrate with existing endpoint management tools of the Bank i.e., (AV, EDR, DLP etc.)	M		
2	Mobile threat Defense Capabilities: a) System Vulnerabilities ➢ Continuously analyze devices to uncover system vulnerabilities. ➢ Automatically mitigate risk until the threat is eliminated. b) Malwares ➢ Automate responses and user notifications with remediation steps to remove the malware. ➢ Dynamically trigger device policy changes in EMM Solution. ➢ Block traffic to malicious server to contain the attack.	O		
Content Management				
1.	Solution should support installing "containerized" apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smart phone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable.	M		
2.	Integrates with existing on-premise repositories.	O		
3.	Content should be encrypted in-motion and at rest	M		
4.	Prevent copy / paste / screenshot / printing	M		
5.	Password protect shared content or encrypt and share content in a secure manner	O		
6.	Limit number of downloads for shared content or control content sharing and access	O		
7.	Block older software versions of apps	M		

Identity Management				
1.	Provides Microsoft AD credential integration	M		
2.	Natively integrates with Microsoft AD Certificate Services	M		
Self Service Portal				
1.	Provide user self-service portal to manage their own devices and corporate access (GPS, Policy and Security Management, Compliance visibility)	O		
2.	Apply privacy settings ensuring sensitive device data is not collected	M		
3.	Self-Service portal/app/ provision to showcase privacy features for end-users and means for users to see what organization can control on device	O		
Secure Browsing				
1.	Provide separate corporate browser for secure browsing.	M		
2.	Intranet browsing through secure tunnel.	M		
3.	Enforce security policies (Prevent copy/paste, Data at rest protection (cache, cookies, history))	M		
4	Provision to whitelist the internal / corporate mobile / Web applications of the Bank on managed / enrolled devices through Secure Tunnel / VPN.	M		

Declaration:

1. We hereby confirm that we have various certificates/bench mark testing standards for the items quoted to meet the intent of the Bid.

2. We hereby confirm that we have back to back arrangements with third party hardware/software for providing continuous and un-interrupted support to meet SLAs obligations as per bid terms.

3. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.

Date:

Signature with seal
Name:
Designation :

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Vertical I.T. Wing, H.O., Bengaluru - 560 001

SECTION F - OWNERSHIP & AWARDING OF CONTRACT

10. Security Deposit / Performance Bank Guarantee

10.1. The successful Bidder should submit a Security Deposit / Performance Guarantee as specified in GeM Bid Schedule within 15 days from the date of acceptance of the Purchase Order.

10.2. If the Security Deposit /Performance Guarantee is not submitted within the time stipulated above, penalty at 0.50% for each completed calendar week of delay or part thereof on the total value of the order will be deducted from the delivery payment or from any other payments for the delay in submission of Bank Guarantee. The total penalty under this clause shall be restricted to 5 % of the total order value.

10.3. Security Deposit should be submitted by way of DD drawn on Canara Bank payable at Bengaluru / Bank Guarantee may be obtained from any of the Scheduled Banks (other than Canara Bank).

10.4. The Bank Guarantee issued by the issuing Bank on behalf of Vendor in favour of Canara Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS). However, it should be as per **APPENDIX-E**. Any bank guarantee submitted in physical mode which cannot be verifiable through SFMS will be summarily rejected.

10.5. Security Deposit/Performance Bank Guarantee should be valid for Total Contract Period from the date of acceptance of order and shall be retained till the completion of Contract period. The guarantee should also contain a claim period of three months from the last date of validity.

10.6. The vendor shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of incompletion of the project and contract period.

10.7. The security deposit / bank guarantee will be returned to the vendor on completion of Contract Period.

10.8. The Bank shall invoke the Bank guarantee before the expiry of validity, if service is not completed and the guarantee is not extended, or if the vendor fails to complete his obligations under the contract.