FORM N: PROPONENT PROPOSAL - REQUIREMENTS

Instructions for filling out Form N: Proponent Proposal - Requirements

1. Complete Form N: Proponent Proposal - Requirements
2. Follow the proposal instructions in the Proposal Instructions section below

PROPOSAL INSTRUCTIONS

1. **For each Mandatory requirement, provide a Y (Yes) or N (No), indicating whether your solution can meet the requirement**. Y indicates that the solution you are proposing will meet the requirements listed in the requirement statement. N indicates that the solution you are proposing will not meet the requirements.

2. **For each Non-Mandatory requirement indicate which Proponent response code that best describes your solution:**

   Y – Available Out of the Box: the solution for the requirement is currently available in the existing product "out of the box". Configuration may be required to enable the feature (requirement will be met through changes to settings of tables, switches, and rules without modification to the source code). Requirement is installed and operational at other sites and can be demonstrated to the City of Winnipeg.

   C – Available via Customization: the solution for the requirement is not currently available in the existing product "out of the box", but may be incorporated via customization of the solution components. Requirement will be met through changes to the source code which would require analysis and re-application during updates, upgrades, or when applying software patches.

   F – Future Availability: the solution for the requirement is not currently available, but will be available in an upcoming planned product release. If this option is indicated, include the date/timeframe when the requirement will be available for implementation, which should be either:
   a) A planned release up to 3 calendar months after the RFP.252-2017 competition close date, where an additional Proponent response code of **3** should be provided;
   b) A planned release up to 6 calendar months after the RFP 252-2017 competition close date, where an additional Proponent response code of **6** should be provided, or
   c) A planned release up to 12 calendar months or longer after the RFP 252-2017 competition close date, where an additional Proponent response code of **12** should be provided.

   3 – Third Party Supplied: the solution for the requirement is expected to be met by using a third party vendor's existing product, either integrated or non-integrated.

   N – Not Possible: the solution for the requirement will not be provided by the Proponent.

3. For each requirement in which the City has noted as "Please Describe", and/or asked specific questions, Bidder shall include additional information, referencing the specific Ref #, at the end of the section and/or as appendices. **Ref # is highly important to ensure linkage between requirement and description.**

Notes:

1. An omitted response will be assumed to be the same as a response code of "N".
2. Any deviation from the response code will be re-coded at the discretion of the City of Winnipeg.

A. Mandatory Requirements				Proponent Response (Y, N)
A1. General Requirements				
Requirement Description	**Requirement Category**	**EMM Requirements Analysis Section#**	**RFQ Requirement Ref#**	
Must provide app code signing capability	General solution requirements		R1	
Must provide app-wrapping capability	General solution requirements		R2	
Must provide app whitelisting and/or blacklisting capability.	General solution requirements		R3	
Must provide web-browsing controls local to device	General solution requirements		R4	
Must be able to manage browser apps	General solution requirements		R5	
Must be centrally managed.	General solution requirements		R6	
Must provide certificate management capability	General solution requirements		R7	
If solution is cloud-based, must have Canadian-based data centers for Production, Development, and Disaster Recovery	General solution requirements		R8	
Must have compliance auditing capability	General solution requirements		R9	
Must have compromise-attempt auditing capability	General solution requirements		R10	
Must have data loss prevention (DLP) capability	General solution requirements		R11	
Must be able to encrypt sensitive corporate data	General solution requirements		R12	
Must be able to enforce compliance rules	General solution requirements		R13	
Must be able to enforce compliance actions	General solution requirements		R14	
Must be able to enforce consistent security policies	General solution requirements		R15	
Must provide FIPS 140-2 validated cryptography	General solution requirements		R16	
Must have asset and inventory	General solution		R17	

management features	requirements			
Must support two-factor or multi-factor authentication	General solution requirements		R18	
Must provide additional security layers for protection of sensitive data	General solution requirements		R19	
Must have Mobile Application Management (MAM) functionality	General solution requirements		R20	
Must have Mobile Content Management (MCM) functionality	General solution requirements		R21	
Must have Mobile Device Management (MDM) functionality	General solution requirements		R22	
Must provide secure Personal Information Management (PIM) functionality	General solution requirements		R23	
Must be able to scale from 250 devices to 4000+ devices	General solution requirements		R24	
Must be able to support internally-developed apps	General solution requirements		R25	
Must be able to block access to consumer app stores	General solution requirements		R26	
Must support all current versions of Microsoft Exchange Server	General solution requirements		R27	
Must be able to access encrypted email and email attachments without use of EMM server	General solution requirements		R28	
Must allow users to access all features of email system including contacts and calendar if EMM server is unavailable	General solution requirements		R29	
Must have capability to support APN setting, passcode policies, activity restriction policies, WiFi settings, Network settings, app updates, OS version management, and security policies through configuration profiles where appropriate to device	General solution requirements		R30	
Must have device location tracking capability	General solution requirements		R31	
Must allow administrators to reset passcodes	General solution requirements		R32	
Must allow administrators to lock/unlock a user	General solution requirements		R33	
Must allow administrators to lock/unlock a device	General solution requirements		R34	
Shall have ability to notify on jailbreak/root detection	General solution requirements		R35	
Shall have Active Directory integration for role/profile management of both end users and support console users	General solution requirements		R36	
Shall have system high availability capability	General solution requirements		R37	

Must have ability to deactivate and reactivate console user accounts and roles	Management Console – console user management		R38	
Must have ability to restrict who can create, delete, and view records	Management Console – console user management		R39	
Must have ability to restrict who can view and delete logs	Management Console – console user management		R40	
Console user IDs must be password protected	Management Console – console user management		R41	
Must support multi-tenancy deployment for governance/data/administrative isolation	Management Console – console user management		R42	
Must support console user templates/profiles (example: administrators, centralized support staff, departmental support staff, report users)	Management Console – console user management		R43	
Shall be able to integrate with Active Directory for sign-on purposes	Management Console – console user management		R44	
Must have ability to deactivate and reactivate device user accounts and roles	Management Console – device user management		R45	
Must have ability to hide/reveal functionality to device user based on permissions	Management Console – device user management		R46	
Must have capability to issue device roaming/geofencing alerts/actions.	Management Console – device user management		R47	
Must support device user templates/profiles (example: administrators, support staff, field staff by business line, office staff)	Management Console – device user management		R48	
Must have anti-virus capability for capable devices.	General endpoint solution requirements		R49	
Must have anti-malware capability	General endpoint solution requirements		R50	
Must have anti-phishing capability	General endpoint solution requirements		R51	
Solution must be device model agnostic	General endpoint solution requirements		R52	
Must support Android devices	General endpoint		R53	

	solution requirements			
Must support iOS devices	General endpoint solution requirements		R54	
Must support Windows 10 devices	General endpoint solution requirements		R55	
Must have Jailbreak/root detection	General endpoint solution requirements		R56	
Must be able to disable/enable the camera	General endpoint solution requirements		R57	
Shall have capability for internal PKI and third-party certificates.	General endpoint solution requirements		R58	
Within the capabilities of specific wireless devices, shall be able to enforce user authentication before device use	General endpoint solution requirements		R59	
Within the capabilities of specific wireless devices, shall be able to configure device lock after exceeding maximum number of failed login attempts	General endpoint solution requirements		R60	
Within the capabilities of specific wireless devices, shall be able to configure device wipe after exceeding maximum number of failed login attempts	General endpoint solution requirements		R61	
Within the capabilities of specific wireless devices, shall be able to configure device lock or wipe if SIM card is changed or removed	General endpoint solution requirements		R62	
Within the capabilities of specific wireless devices, shall be able to disable use of removable media	General endpoint solution requirements		R63	
Within the capabilities of specific wireless devices, shall be able to disable device voice control	General endpoint solution requirements		R64	
Within the capabilities of specific wireless devices, shall be able to control which apps can access data on device	General endpoint solution requirements		R65	
Within the capabilities of specific wireless devices, shall be able to control “screenshot” ability	General endpoint solution requirements		R66	
Within the capabilities of specific wireless devices, shall be able to control printing ability	General endpoint solution requirements		R67	
Within the capabilities of specific wireless devices, shall be able to prevent sideloading of apps	General endpoint solution requirements		R68	
Within the capabilities of specific wireless devices, shall be able to prevent use of AirDrop, Android Beam, and Wi-Fi direct and like-technology	General endpoint solution requirements		R69	
Must be able to alert end user when	General end-user		R70	

roaming	experience requirements			
Must provide secure access to Corporate data	General end-user experience requirements		R71	
Must provide premium 24/7 support with a 30-minute response time	Vendor support		R72	
Must be able to provide a product roadmap with lifecycle dates for major releases	Vendor support		R73	
Must be able to provide a minimum of one year of retirement support for on-premises solutions	Vendor support		R74	

B. Non-Mandatory Requirements				Proponent Response (Y, C, F, 3, N)
B1. General Requirements				
Requirement Description	**Requirement Category**	**EMM Requirements Analysis Section#**	**RFQ Requirement Ref#**	
Should have ability to automatically send email	General solution requirements		R75	
Should have ability to automatically send SMS	General solution requirements		R76	
Should have ability to log end-user acknowledgements	General solution requirements		R77	
Should have ability to log end-user notifications	General solution requirements		R78	
Should have ability to log support user acknowledgements	General solution requirements		R79	
Should have ability to log support user notifications	General solution requirements		R80	
Should have ability to provide notifications to support user	General solution requirements		R81	
Should have ability to require acknowledgement by support user	General solution requirements		R82	
Should have Active Directory integration for devices	General solution requirements		R83	
Should allow app deployment based on user role/profile	General solution requirements		R84	
Should be able to create app groupings based on device OS	General solution requirements		R85	
Should have API for integration with other systems	General solution requirements		R86	
Should have API or webservice for device location exporting	General solution requirements		R87	
Should provide cloud repository access and the ability to manage it *Please describe.*	General solution requirements		R88	
Should permit custom reporting	General solution requirements		R89	
Should be able to export data to reporting software (example: Crystal Reports)	General solution requirements		R90	
Should be able to provide on-demand listing of devices and users	General solution requirements		R91	
Should be able to provide report to show PCI DSS compliance	General solution requirements		R92	
Should have device retention policy management functionality	General solution requirements		R93	
Should provide Digitial Rights Management (DRM) for documents	General solution requirements		R94	

Should support on-device event triggers	General solution requirements		R95	
Should support event triggers based on external events such as vulnerability discovery	General solution requirements		R96	
Should support event-based workflow triggers	General solution requirements		R97	
Should have feature parity if offering both cloud-based and on-premise solutions	General solution requirements		R98	
Should support Group Policy integration	General solution requirements		R99	
Should be able to integrate with Network Access control (NAC) systems	General solution requirements		R100	
Should be able to manage profiles for Cisco and f5 VPNs	General solution requirements		R101	
Should be able to integrate with Symantec Endpoint solution	General solution requirements		R102	
Should be able to integrate with Peoplesoft, including automatic actions on employment status changes	General solution requirements		R103	
Should protect privacy through configurable settings, such as application inventory and physical location tracking, for BYOD deployments	General solution requirements		R104	
Should have proxy integration capability	General solution requirements		R105	
Should have record retention policy management capability	General solution requirements		R106	
Should be able to integrate with Remedy solution	General solution requirements		R107	
Should provide an internal incident management system			R108	
Mobile Device Management should be separate from Mobile Application Management	General solution requirements		R109	
Should provide server storage usage alerting	General solution requirements		R110	
Should support secure data distribution	General solution requirements		R111	
Should support shared devices	General solution requirements		R112	
Should be able to provide alerting on users congregating	General solution requirements		R113	
Should provide a user self-service portal	General solution requirements		R114	
Should have zero-day support for new operating systems and devices	General solution requirements		R115	
Should have support for Apple’s Device Enrollment Program	General solution requirements		R116	
Should support Apple Volume Purchase Program	General solution requirements		R117	

Should have ability to manage wi-fi only devices	General solution requirements		R118	
Should be able to remove managed apps from device when management ceases	General solution requirements		R119	
If on-premise hosted, should be able to run in a virtualized environment	General solution requirements		R120	
Should be able to report annual and monthly metrics - # of devices	Metrics		R121	
Should be able to report annual and monthly metrics – app usage	Metrics		R122	
Should be able to report annual and monthly metrics – by department	Metrics		R123	
Should be able to report annual and monthly metrics – by end user-role	Metrics		R124	
Should be able to report annual and monthly metrics – data usage	Metrics		R125	
Should be able to report annual and monthly metrics – SMS usage	Metrics		R126	
Should be able to report annual and monthly metrics – voice usage	Metrics		R127	
Should support role-based security	Management Console – console user management		R128	
Should have ability to hide/reveal functionality to console user based on permissions	Management Console – console user management		R129	
Should have ability to provide notifications to end-users and/or user groups	General endpoint solution requirements		R130	
Should have ability to require acknowledgement by end-user	General endpoint solution requirements		R131	
Should be able to perform automated action	General endpoint solution requirements		R132	
Should have lone worker check-in capability	General endpoint solution requirements		R133	
Should support copy/paste, editing, sharing, and saving controls *Please describe.*	General endpoint solution requirements		R134	
Should support custom alerts	General endpoint solution requirements		R135	

Should be able to provide access based on device location (example: at office vs at home)	General endpoint solution requirements		R136	
Should support "man down" capability	General endpoint solution requirements		R137	
Should have capability to separate corporate and personal data	General endpoint solution requirements		R138	
Should support integration with Internet of Things (IoT)	General endpoint solution requirements		R139	
Should support Mac OSX devices	General endpoint solution requirements		R140	
Should support Windows CE devices	General endpoint solution requirements		R141	
Should support Windows Mobile devices	General endpoint solution requirements		R142	
Should support Windows Phone devices	General endpoint solution requirements		R143	
Should support Blackberry devices	General endpoint solution requirements		R144	
Should be able to provide access based on current time (example: no access after 5pm to corporate documents)	General endpoint solution requirements		R145	
Should provide workflow capability.	General endpoint solution requirements		R146	
Should be able to support CIFS data shares	General endpoint solution requirements		R147	
Should have ability to electronically sign documents	General end-user experience requirements		R148	
Should have ability to annotate PDF documents	General end-user experience		R149	

	requirements			
Should have a branded app store	General end-user experience requirements		R150	
Should have capability for device check-out/check-in for shift workers or shared devices	General end-user experience requirements		R151	
Should have file editing collaboration capability	General end-user experience requirements		R151	
Should have file multi-user access capability	General end-user experience requirements		R153	
Should provide online self-support for at least five years after release retirement for on-premises solution.	Vendor support		R154	