TERMS OF REFERENCE

PROCUREMENT OF REMOTE MONITORING AND MANAGEMENT

The New Normal has brought challenge to all private and government organizations. It changed the landscape of how business is conducted, clienteles are reached, and operations are being supported. An important element of this new landscape is having a pro-active and responsive Information Technology (IT) group.

Since majority of the workload, meetings and decisions are all driven and influenced by technology this time of pandemic, ERC's IT group must use new technologies to support the agency's entire operation.

A Remote Monitoring and Management (RMM) tool is an application to address both office and work-from-home setups; managing all IT assets, supporting your workforce, proactively monitoring the entire system, and knowing and preventing the problem even before it happens.

RMM is a compendium of software solutions rolled into one and its generally highlighted features are as follows:

- Endpoint Management
- Patch Management
- Compliance and Security
- Network Monitoring
- Automation and Scripting
- Asset Management
- Reporting Tool
- Mobile App
- User Admin
- Remote Access
- Integrations and many more.

The Energy Regulatory Commission (ERC) is developing its capabilities in providing a robust RMM to improve visibility and monitoring its networking assets.

As the ERC's ICT infrastructure and systems continue to expand, there is a greater need to be able to efficiently monitor and maintain its network resources across ERC offices. An RMM will allow the ERC

to remotely monitor and manage its various network equipment and peripherals.

I. PROJECT COVERAGE

The scope of services covers the following:

1. Supply, delivery and installation of the RMM Tool to ERC;
2. Compliance to Section 6 (Scope of Work);
3. Compliance to Section 7 (Service Level Agreement);
4. Five (5) days extensive technical training; and
5. Provision of one (1) year updates and onsite/online technical support.

II. CONTRACT PERIOD

The delivery period shall be twenty-one (21) days from **receipt of Notice to Proceed (NTP)** including the five (5) days extensive technical training. The contract period for the Subscription of Managed Services (Remote Monitoring and Management) shall be **twelve (12) months** from the date of full delivery of the RMM Tool.

III. APPROVED BUDGET FOR THE CONTRACT

1. Fund for this engagement shall be sourced from the Current Appropriation for the fiscal year 2021 of the ERC.

2. The ABC for the project is **THREE MILLION PESOS (PhP3,000,00.00)** inclusive of all applicable government taxes, other fees, and charges.

IV. MODE OF PROCUREMENT

The Mode of Procurement shall be **Competitive or Public Bidding,** as specified in the 2016 IRR of Republic Act (RA) No. 9184. Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country that the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

V. QUALIFICATIONS

The service provider should have the necessary eligibility, experience, and expertise in providing the RMM Tool:

1. The bidder shall submit a valid and current Certificate of Distributorship/Dealership/Resellership of the product being offered, issued by the principal or manufacturer of the product (if bidder is not the manufacturer). If not issued by manufacturer, must also submit certification/document linking bidder to the manufacturer.
2. The bidder shall have at least one (1) personnel that can support the solution being offered with a certification.
3. Must comply with imposed health protocols. Service providers must have a valid swab test result issued within three (3) days before proceeding onsite and must fill up a health declaration form before entering the ERC premises. Wearing of face masks and face shields are a must. Those who have COVID-19 symptoms shall be refused entry.

VI. SCOPE OF WORK

Supply, delivery, and installation of the RMM Tool to ERC with the following requirements:

1. Technical Specifications

ITEM	SPECIFICATIONS
RMM Tool and Network Management System	500 Licenses for Network Monitoring and RMM
PERFORMANCE AND NETWORK MONITORING	
General Features	Solution should be able to monitor processes and services
	Solution should be able to monitor system performance such as CPU, Memory, Disk and Bandwidth Utilization
	Solution should be able to monitor hardware and software changes via reports
	Solution should be able to monitor IP devices uptime and downtime
	Solution should be able to monitor Windows, VMware, Mac and Linux
	Solution should be able to trigger an alarm, send an email and run a procedure when an alert is detected
	Solution supports Port status, port map monitoring, and SNMP traps
	Solution should identify device roles automatically; identified based on device characteristics

	Supports NetFlow, jFlow, sFlow, IPFIX
	Solution should be able to display monitoring in a dashboard
	Solution should be able to provide reports of triggered alerts
Provides user defined real-time monitoring	Alerts
	Event Log Alerts
	Monitor sets
	SNMP sets
	System check
	Log monitoring
	Monitoring of IP Devices
	Monitors changes in the configuration of IT system
	Provides alerts via SMS, email, dashboard or run a procedure.
	Monitor devices online/offline status
	Monitor system performance (CPU, Disk Space, Memory)
	Monitor Processes
	Monitor Services
	Monitor Hardware and Software Changes via reports
	Alert message and recipient configuration
Automated Network Discovery	Automatically discover all network devices
Dashboard	Offers view of alerts summary per system (device)
	Ability to group systems together
	Customize alerts
AGENT DEPLOYMENT	
Deployment	Deploy Agent Remotely thru Active Directory or any third party application
	Deploy Agent via URL Link
Agent Installer	Can Bind Administrator Credential inside the Agent package once installed
	Can group machine base in agent package
SUPPORTED DEVICES	
Workstations, Servers Platform supported	Windows 8/8.1/10
	Windows Server 2008/2008 R2/2012/2012 R2/2016
	Apple OS X version 10.7.5 through 10.9 or above. Intel only
	Network Devices – Routers, Switches, Printers and other IP-based devices
	Any SNMP enabled device
	Supports Linux Debian, RPM
AGENT PROCEDURE	
Procedure Creation	Create IT Procedures/Scripts.
	Automatically distribute procedures to manage machines, groups of machines within a Local Area Network and/or Remote systems.

	Able to run CMD, PowerShell, Batch File, VB script commands, Javascript
Automated Remediation	Automatically run procedures triggered by an alert (via Real-time monitoring of critical applications, services, event logs) offering automated remediation of issues.
Scheduling	Schedule procedures to run automatically
Application Deployment	Deploy Microsoft and non-Microsoft applications
Policy Enforcement/ Configuration Management	Deploy and enforce system policies, configuration, e.g. block control panel, block USBs via Machine, groups of Machine within a Local Area Network and Remote systems.
INVENTORY, ASSET DISCOVERY AND AUDIT	
Offers comprehensive audit of each system – Hardware, Software Inventory.	
Hardware Inventory	Solution should be able to take inventory of hardware information such as:
	System Information (Manufacturer, Product Name, System Version)
	Chassis (Chassis Manufacturer, Chassis Version, Chassis Serial Number, Chassis Asset Tag)
	Network Information (IPv4 Address, IPv6 Address, Subnet
	Mask, Default Gateway, Connection Gateway, IP
	MAC Address, DHCP Server, DNS Server
	Motherboard (Manufacturer, Version, Serial Number)
	BIOS Information (Vendor, Version, Release Date)
	CPU/RAM Information (Processor Manufacturer, Processor Family, Processor Version, CPU Max Speed, CPU Current Speed, CPU, Quantity, Speed, RAM, Max Memory Size, Max Memory Slots)
	On Board Devices
	Memory Devices per Slot
	System Slots
	SNMP enabled Printers Installed on the system
	Disk Hardware
	Disk Volumes
	Disk Partitions
Software inventory	Solution should be able to provide inventory of software information such as
	Software Licenses (Publisher, Title, Product Key, License Key, Version)
	Installed Applications (Application, Description, Version, Manufacturer, Product Name)
	Add/Remove (Application Name)
	Security Products (Product Type, Product Name, Active, Up to Date)

System Information	Solution should be able to inventory system information such as
	IP information
	Disk volume information including drive letters
	Space available, volume labels
	Drive hardware information including models and user.
	CPU and RAM information with specifics on, CPU speeds, models, number, and ram installed,
	Printer information
PATCH MANAGEMENT	
General Features	System Compatibility. Whether the application is agent-based or agent-less it should have a less impact on the performance, stability and compatibility with the current operating environment especially if this will be deployed across a large number of assets or machines.
	Cross-platform support to patch Windows and Mac operating systems.
	Ease of deployment and maintenance. The easier the patch management solution is to deploy and maintain, the lower the implementation and ongoing maintenance costs to the organization.
	Solution should be able to support non-Microsoft products for patching and is able to do seamless deployment of patches – similar approach to a Microsoft application.
	Solution should be able to automatically download Internet Based patches without worrying network congestion, even machines without direct access to Microsoft.
	Solution should be able to support patching heterogeneous endpoints such as laptops, desktops, servers, and virtual machines.
	Solution should have the capability to select type of patch to be downloaded (Critical, Security, hotfix, etc.)
	Solution should have the capability to schedule a workstation/server reboot whenever patch requires a reboot.
	Solution should be able to completely automate patching process.
	Solution should be able to revert deployed patch. Via restore point
	Solution has the capability to create patch groups
	Solution should be able to create test groups to test patches on a small number of endpoints before approving them for deployment.
	Solution should provide alerts via dashboard
	Solution should provide description of the patch
	Solution should be able to notify users about patch deployment via notification window

	Audit Trail and Report. The solution should be able to provide a comprehensive logging facility.
	Reports should be readily available on an on-demand or per need basis that will help the administrator keep track of the status of software fixes and patches on individual systems. Report can also be customized, or tailored fit based on the requirement on-hand. Solution should provide reports not limited to updated and outdated endpoints, successful and unsuccessful patch count, patch status per endpoint or per group/batch etc.
Manage Machines	Offers Scan machine, Patch status, Schedule scan, Initial and automatic updates, Pre/Post procedure, Machine History
Manage Updates	Ability to Machine/Patch updates,
	Provides Rollback via restore-point
	Reject Updates
Patch Policy	Create/Delete Policies
	Approval by Policy
	Knowledge Based Override
Automatic and recurring patch scans	Secured or ad-hoc, Scans networks for installed and missing security patches, detects vulnerability, determines which patches are needed.
	By computer, group or user defined collections of computers
	Automates the tedious process of researching, identifies which patches are installed and date installed, Monitors and maintains patch compliance for entire enterprise
Centralized Management of Patches	Does not require multiple patch servers
	Ensures that all systems are protected, even remote users on laptops and workstations
	Allows implementation across entire network
	Always know what patches and security holes reside on each user's system
Patch approval	Approve or deny selected patches
	Select by user defined computer collections
Automated patch deployment	Schedule by time, computer, group or user defined collections of computers
	Simultaneously deploy all required patches across operating systems
	Single rollout strategy and policy enforcement
	Maximize uptime
Interactive patch management	Select to deploy by patch or by computer
	Select individual computers, groups or user defined collections of computers
	Ad-hoc simultaneous deployment of selected patches
	Across operating systems
	Across locations

Flexible configuration	Patch file location, Patch file parameters
	Reboot actions and notifications, By computer, group or user defined collections of computers
	Security and policy control
Comprehensive reports	Graphical with drill-down, User defined
	Scheduled, E-mail notification
	Export to HTML, Excel or PDF
	Solution should be able to run procedures triggered by an alert (via real-time monitoring of critical applications, services, event logs) offering automated remediation of issues
	Solution should be capable to create customized IT Procedures
	Solution should be able to support execution of CMD, Powershell, Batch File and VB Script
	Solution should be able to easily deploy 3rd party applications
Cross-platform support	Windows
	MAC
	Patches for 3rd party software is included, if made available by 3rd-party software package developers
Profile base policy	Scan
	3rd-Party Software
	Deployment
	Alerting thru dashboard
Scan and Analysis	Can Approve, Review and Reject Patch
	Schedule (Daily, Weekly, Monthly)
Override	Can Approve/Reject Specific KB Override
	Can Approve/Reject Specific MS Override
	Can Approve/Reject Specific CVE, Product, or Vendor
3rd-Party Software	Deploy popular 3rd-party software packages for Windows systems
	Reboot Options
Deployment	Warn user and wait for x min and then reboot
	Reboot immediately after update
	Ask user about reboot and offer to delay
	Skip reboot
	Schedule: Daily, Weekly, Monthly
Alerting	New patch is availability thru dashboard and OS Patches
	Deployment fails
	Create Alarm
	Email Recipients
Management	Dashboard
	Patch Approval
	Patch History

REMOTE ACCESS	
General Features	Solution should be capable of remoting a managed machine
	Solution should be able to set remote control policies such as Silent take control, ask permission, approve if no one is logged in
	require permission, denied if no one is logged in
	Solution should be able to record a remote session
	Solution should be able to access the command prompt without disturbing the user
	Solution should be able to access and modify the registry, services and processes without disturbing the user
	Solution should be able to get audit information of the remote system without disturbing the user
	Can do remote using a mobile application
Capability to access remote systems without disturbing the user	Access to Command Prompt
	Access to Asset Summary
	Access to Registry
	Access File Manager (Download, Rename, Delete, Move, Copy,
	Upload)
	Access to Task manager
	Access to Processes
	Access to Services
	Easy administration of users and policies
	Access computers from anywhere
	Access computers from anywhere
	Private Remote-Control Session for Windows
	Remote Control Session is Logged
	Supports Multiple Monitors
	Supports Keyboard Mapping and Short-cut
	Secure Communications
	Provide the end user control and security to enable or disable remote control functions until granted approval
REPORT and ALERTING	
	Detailed list, table and graphic style reports
	Hardware and Software Inventory
	Disk Utilization
	License Usage and Compliance
	Network Usage and Statistics
	Schedule Reports for Automatic Distribution
	Distribute automatically to selected e-mail recipients
	Report for all, groups or specific computers
	Detailed filtering and content selection
	Add own logo
	Save reports with selected parameters for reuse
	Export report data to readable formats
	Capable of sending SMS Notifications with no extra cost via a built-in SMS gateway avoiding delays from integrations; at the

	very least a minimum of 1.1 million SMS per month or a total of 13.2 million SMS for 1 year but should be able to provide more if needed.
	Capable of email and mobile app notifications
TICKETING	
General Features	Have a main Resolver
	Single-pane RMM integration
	Can create end-user ticket requestor
	Can manage the status of the ticket
	Can set status new
	Can set status open
	Can set status waiting
	Can set status pause
	Can set status resolved
	Create ticket using email
	Can add contacts by registering email addresses
	Can send real time updates thru active chat
	Can set priorities to low, medium, high or none
	Can copy furnish email addresses for monitoring
	Can set ticket type whether problem, question, incident, task, or none
	Can delegate ticket assignee
	Can set severity of the ticket
	Can search ID number of tickets
	Capable of automatic resolution of tickets
	Viewable source of the tickets
	Have searchable filters such as ticket ID, organization, requestors, priority, severity, status, date and tags
	Automatic identification of device requestor
	Customizable organization structures of requestor
	Can set tags of the ticket
	Capable of public and private replies
	Can see the logs of the ticket
	Can attach file on the ticket
	Can add a link on the ticket
	Can set location or department
	Can see the deleted tickets
	Can View my tickets
	Can view all open tickets
	Can view unassigned tickets
	Can view, reject, and approve pending tickets sent via email
	Can create and customize domain for ticketing service
	Can configure timeframe for “resolved tickets” to “close” status
	Can configure SLA timers

	Configurable start of ticket numbers
	Allow endusers and contacts to attach files on the ticket
	Allows options for authentication to view attached file in the ticket
	Configurable technical email response either public or private
	Can configure systray help request
	Can set and file event-based triggered tickets
	Can set and file time based triggered tickets
	Can create ticket forms
	Can generate reports
	- open ticket reports
	- resolution time reports
	- technician ticket efficiency report
	- ticket volume report
ADMINISTRATION	
General Feature	Solution should be able to limit the access to its module and visibility of machines per user
	Solution should be able to propagate policies automatically without further user intervention once policies are assigned to machines, machine group or organization
	Solution should be able to provide compliance reports of enforced securities and policies
Access Management	Multi-tenant Capable
	Ability to group systems
	Assign Admin users
	Ability to assign roles, scope and groups to Admin Users
	Logs activities of Users using the system
	Ability to access Admin system remotely
Centralized Management	Ability to manage, monitor local and remote systems in a single console (without the need for a private connectivity).
	Ability to deploy policies, monitoring definitions to both local and remote systems using a single console.
System Security	Compliance to HIPAA and CCPA
	Remote control sessions to end-user machines/servers are encrypted
	Access to the user and admin web interface is encrypted using industry accepted standards
	Capable of 2 factor authentication
Accessibility	
Ease of Access	Accessible thru the program's web-based application
	Accessible thru the program's mobile application (mobile app for iOS and Android)
SUPPORT	
	1 year of updates and support
Local Support	9 x 5 Phone, Onsite, E-mail and Chat support, One (1) hour response time upon receipt of call

2. Technical Manuals and Trainings:

a. RMM Tool Manual;
b. Frequently Asked Questions (FAQs) on the RMM Tool; and
c. Five (5) days extensive technical training.

Summary of Deliverables:

- Supply, delivery and installation of the RMM Tool to ERC;
- Compliance to Section 6 (Scope of Work);
- Compliance to Section 7 (Service Level Agreement);
- Provision of Technical Manual(s) and FAQs;
- Five (5) days extensive technical training; and
- Provision of one (1) year updates and onsite/online support.

VII. SERVICE LEVEL AGREEMENT

1. ERC shall maintain a Service Level Agreement (SLA) with the Service Provider, subject to Section 10 (Liquidated Damages) for their non-compliance. The terms and conditions of the SLA are enumerated below:

Criteria	Description
1.1. System Maintenance and Support	Provide 9 (hours) X 5 (days) technical support on the problems reported by ERC based on the prescribed time frames
1.2. Software updates, maintenance releases and patches	Provide software updates, maintenance releases and patches within thirty (30) calendar days after product distribution in the market for the duration of the contract at no additional cost to the ERC.

2. The Service Provider shall give ERC support (online and offsite) during the contract period.

VIII. CONFIDENTIALITY OF DATA

The Service Provider shall maintain confidentiality on information gathered or gained access during the delivery and

contract period. Thus, release of data or any information regarding thereto shall require consent from the ERC.

IX. TERMS OF PAYMENT

1. The Total Contract Price should not exceed the ABC of THREE MILLION PESOS (PhP3,000,000.00). Payment shall be released within thirty (30) days after the completion of delivery of the item and final acceptance at the ERC Main Office and submission of the required documents.
2. Since the above payment shall be subject to the usual government accounting and auditing requirements, the Winning Bidder is expected to be familiar with the Government Accounting and Auditing Manual (GAAM).

X. LIQUIDATED DAMAGES

1. Where the Software Vendor refuses or fails to satisfactorily complete the work within the specified contract time, plus any extension time duly granted and is hereby in default under the contract, the Software Vendor shall pay ERC for liquidated damages, and not by way of penalty, an amount, as provided in the conditions of the contract, equal to one tenth (1/10) of one percent (1%) of the cost of the unperformed portion for every day of delay. The maximum deduction shall be ten percent (10%) of the amount of the contract, of which ERC may rescind or terminate the contract, without prejudice to other courses of action and remedies available under the circumstances such as but not limited to forfeiture of performance security and/or blacklisting of the latter.
2. For entitlement to such liquidated damages, ERC need not prove the damages actually incurred. Said damages in any amount shall be deducted from any money due or which may become due the Software Vendor under the Contract and/or collect such liquidated damages from the retention money or other securities posted by the Software Vendor at ERC's convenience.

XI. RESERVATION CLAUSE

The ERC reserves the right to accept or reject any quotation, to annul the procurement process, and to reject all quotations at any time without thereby incurring any liability to the affected supplier/s.