

# **TERMS OF REFERENCE**

## **Endpoint Desktop Management System**

### **Background:**

The Office of the Solicitor General is developing its capabilities in providing a robust **ENDPOINT DESKTOP MANAGEMENT SYSTEM** to improve visibility and monitoring its IT assets.

As the Office of the Solicitor General's ICT infrastructure and systems continue to expand, there is a greater need to be able to efficiently monitor and maintain its ICT resources from both in the central command in Makati and its remote operations. An Endpoint Desktop Management System will allow the Office of the Solicitor General to effortlessly and remotely monitor and manage its various endpoints including desktops and laptops.

### **Objective:**

The Office of the Solicitor General requires an **ENDPOINT DESKTOP MANAGEMENT SYSTEM** to support monitoring, policy enforcement, inventory & compliance audit, patch management, software management, remote access support, ticketing and reporting.

To meet its objective, the Office of the Solicitor General seeks to acquire a comprehensive Endpoint Desktop Management System.

Approved budget for this project is Two Million Pesos (Php 2,000,000.00).

### **For the procurement of Endpoint Desktop Management System:**

1. The bidder must have completed, within the last 3 years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC; or the prospective bidder should have completed at least two (2) similar contracts and the aggregate contract amounts should be equivalent to at least fifty percent (50%) of the ABC; and the largest of these similar contracts must be equivalent to at least half of the fifty percent (50%) of the ABC as required.

2. 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.
3. The bidder shall have at least one (1) personnel that can support the solution being offered with a certification.

**Endpoint Desktop Management System Technical Specifications:**

ITEM	QTY	UNIT COST	TOTAL
Endpoint Desktop Management System with Access License for 600 units	1 Lot	2,000,000.00	2,000,000.00
<b>SUB TOTAL</b>			<b>₱ 2,000,000.00</b>

ITEM	SPECIFICATION
<b>AGENT DEPLOYMENT</b>	
<b>Deployment</b>	<ul style="list-style-type: none"> <li>• Deploy Agent Remotely thru IP Address</li> <li>• Deploy Agent Remotely thru Active Directory</li> <li>• Deploy Agent thru Discovery</li> <li>• Deploy Agent via URL Link</li> </ul>
<b>Agent Installer</b>	<ul style="list-style-type: none"> <li>• Can Bind Administrator Credential inside the Agent package</li> <li>• Can Automatically group machine base in Agent package</li> <li>• Agent Icon can be hidden or change to reflect OSG logo</li> </ul>
<b>SUPPORTED DEVICES</b>	
<b>Workstations, Servers Platform supported</b>	<ul style="list-style-type: none"> <li>• Windows XP/Vista/7/8/8.1/10</li> <li>• Windows Server 2003/2008/2008 R2/2012/2012 R2/2016</li> <li>• Virtualization - VMWare/Hyper-V</li> <li>• Apple OS X version 10.7.5 through 10.9 or above. Intel only</li> <li>• The Linux agent only supports Intel-based machines. SuSE Linux Enterprise (10, 11, 12), Red Hat Enterprise Linux (5, 6, 7), Ubuntu (10.04 LTS, 12.04 LTS, (16.04 LTS) are supported as a headless agent. User interface-based agent procedures will not work. OpenSuSE 12, and CentOS (5, 6, 7) are fully supported.</li> <li>• Network Devices - Routers, Switches, Printers and other IP-based devices.</li> </ul>

ITEM	SPECIFICATION
<b>AGENT PROCEDURE</b>	
<b>Procedure Creation</b>	<ul style="list-style-type: none"> <li>• Create IT Procedures/Scripts.</li> <li>• Automatically distribute procedures to manage machines, groups of machines within a Local Area Network and/or Remote systems.</li> <li>• Able to run CMD, PowerShell, Batch File, VB script commands</li> </ul>
<b>Automated Remediation</b>	<ul style="list-style-type: none"> <li>• Automatically run procedures triggered by an alert (via Real-time monitoring of critical applications, services, event logs) offering automated remediation of issues.</li> </ul>
<b>Scheduling</b>	<ul style="list-style-type: none"> <li>• Schedule procedures to run automatically</li> </ul>
<b>Application Deployment</b>	<ul style="list-style-type: none"> <li>• Deploy Microsoft and non-Microsoft applications</li> <li>• Capability to assign software repository for local sourcing of installers.</li> </ul>
<b>Policy Enforcement/Configuration Management</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>File Distribution</b>	<ul style="list-style-type: none"> <li>• Automatically get and distribute files to and from systems connected locally and remotely.</li> </ul>
<b>PERFORMANCE AND NETWORK MONITORING</b>	
<b>General Features</b>	<ul style="list-style-type: none"> <li>• Solution should be able to monitor processes and services</li> <li>• Solution should be able to monitor system performance such as CPU, Memory, Disk and Bandwidth Utilization</li> <li>• Solution should be able to monitor hardware and software changes</li> <li>• Solution should be able to monitor IP devices uptime and downtime</li> <li>• Solution should be able to monitor Windows, VMware, Linux, Cisco IOS and 20 other operating systems covering a wide range of networking devices, web, database and email servers, log files and Windows performance counters.</li> <li>• Solution should be able to trigger an alarm, file a ticket, send an email and run a procedure when an alert is detected</li> <li>• Solution should be able to display monitoring in a dashboard</li> <li>• Solution should be able to provide reports of triggered alerts</li> </ul>
<b>Provides user defined real-time monitoring</b>	<ul style="list-style-type: none"> <li>- Alerts</li> <li>- Event Log Alerts</li> </ul>

ITEM	SPECIFICATION
	<ul style="list-style-type: none"> <li>- Monitor sets</li> <li>- SNMP sets</li> <li>- System check</li> <li>- Log monitoring</li> </ul>
	<ul style="list-style-type: none"> <li>• Monitoring of IP Devices</li> <li>• Monitors changes in the configuration of IT system and provides alerts if a change has occurred.</li> <li>• Provides alerts via tickets, email, dashboard or run a procedure.</li> <li>• Alert on specific file changes and protection violations.</li> <li>• Monitor devices online/offline status</li> <li>• Monitor system performance (CPU, Disk Space, Memory)</li> <li>• Monitor Processes</li> <li>• Monitor Services</li> <li>• Monitor Hardware and Software Changes</li> <li>• Alert message and recipient configuration</li> </ul>
<b>Automated Network Discovery</b>	<ul style="list-style-type: none"> <li>• Automatically discover all devices on the network</li> <li>• LAN monitoring alerts when new devices are detected</li> <li>• View all known and unknown devices</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Offers view of alerts summary per system (device)</li> <li>• Ability to group systems together</li> <li>• Customize alerts</li> <li>• Offers Multi Router Traffic Grapher (MRTG), Bandwidth consumption.</li> </ul>
<b>INVENTORY, ASSET DISCOVERY AND AUDIT</b>	
	<b>Offers comprehensive audit of each system - Hardware, Software Inventory.</b>
<b>Hardware Inventory</b>	<ul style="list-style-type: none"> <li>• Solution should be able to inventory hardware information such as: <ul style="list-style-type: none"> <li>- System Information (Manufacturer, Product Name, System Version, System Serial Number)</li> <li>- Chassis (Chassis Manufacturer, Chassis Type, Chassis Version, Chassis Serial Number, Chassis Asset Tag)</li> <li>- Network Information (IPv4 Address, IPv6 Address, Subnet Mask, Default Gateway, Connection Gateway, Country, IP Information Provider, MAC Address, DHCP Server, DNS Server)</li> <li>- Motherboard (Manufacturer, Product, Version, Serial Number, External Bus Speed)</li> <li>- BIOS Information (Vendor, Version, Release Date)</li> </ul> </li> </ul>

ITEM	SPECIFICATION
	<ul style="list-style-type: none"> <li>- 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)</li> <li>- On Board Devices</li> <li>- Port Connectors</li> <li>- Memory Devices per Slot</li> <li>- System Slots</li> <li>- Printers Installed on the system</li> <li>- PCI and Disk Hardware</li> <li>- Disk Volumes</li> <li>- Disk Partitions</li> <li>- Disk Shares</li> </ul>
<b>Software inventory</b>	<ul style="list-style-type: none"> <li>• Solution should be able to inventory software information such as <ul style="list-style-type: none"> <li>- Software Licenses (Publisher, Title, Product Key, License Key, Version)</li> <li>- Installed Applications (Application, Description, Version, Manufacturer, Product Name, Directory Path, File Size, Last Modified)</li> <li>- Add/Remove (Application Name, Uninstall String)</li> <li>- Startup Apps (Application Name, Application Command, User Name)</li> <li>- Security Products (Product Type, Product Name, Manufacturer, Version, Active, Up to Date)</li> </ul> </li> </ul>
<b>System Information</b>	<ul style="list-style-type: none"> <li>• Solution should be able to inventory system information such as <ul style="list-style-type: none"> <li>- IP information</li> <li>- DNS/DHCP server information</li> <li>- Disk volume information including drive letters</li> <li>- Space available, volume labels</li> <li>- PCI and drive hardware information including models, and user editable notes for each device</li> <li>- CPU and RAM information with specifics on, CPU speeds, models, number, and ram installed,</li> <li>- Printer information with Name, Port and Model</li> </ul> </li> </ul>
<b>Custom Fields</b>	Can add additional information Manually or Automatically
<b>PATCH MANAGEMENT</b>	
<b>General Features</b>	<ul style="list-style-type: none"> <li>• 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</li> </ul>

ITEM	SPECIFICATION
	<p>environment especially if this will be deployed across a large number of assets or machines.</p> <ul style="list-style-type: none"> <li>• Cross-platform support to patch Windows and Mac operating systems.</li> <li>• 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.</li> <li>• 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.</li> <li>• Solution should use peer to peer technology in deploying patches</li> <li>• Solution should be able to automatically download Internet Based patches without worrying network congestion, even machines without direct access to Microsoft.</li> <li>• Solution should be able to support patching heterogeneous endpoints such as laptops, desktops, servers, and virtual machines.</li> <li>• Solution should have the capability to select type of patch to be downloaded (Critical, Security, hotfix, etc.)</li> <li>• Solution should have the capability to schedule a workstation/server reboot whenever patch requires a reboot.</li> <li>• Solution should be able to completely automate patching process.</li> <li>• Solution should be able to revert deployed patch.</li> <li>• Solution has the capability to create patch groups</li> <li>• Solution should be able to create test groups to test patches on a small number of endpoints before approving them for deployment.</li> <li>• Solution should be able to throttle bandwidth when downloading patch to workstations/servers.</li> <li>• Solution should provide alerts / warnings like or not limited to email notification for new patches</li> <li>• Solution should be able to monitor direct patch fix of applications on the server.</li> <li>• Solution should provide description of the patch</li> <li>• Solution should be able to notify users about patch deployment via notification window</li> <li>• Audit Trail and Report. The solution should be able to provide a comprehensive logging facility.</li> </ul>

ITEM	SPECIFICATION
	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>Manage Machines</b>	<ul style="list-style-type: none"> <li>• Offers Scan machine, Patch status, Schedule scan, Initial and automatic updates, Pre/Post procedure, Machine History</li> </ul>
<b>Manage Updates</b>	<ul style="list-style-type: none"> <li>• Ability to Machine/Patch updates,</li> <li>• Provides Rollback</li> <li>• Cancel Updates</li> </ul>
<b>Patch Policy</b>	<ul style="list-style-type: none"> <li>• Create/Delete Policies</li> <li>• Approval by Policy</li> <li>• Knowledge Based Override</li> </ul>
<b>Automatic and recurring patch scans</b>	<ul style="list-style-type: none"> <li>• Secured or ad-hoc, Scans networks for installed and missing security patches, detects vulnerability, determines which patches are needed.</li> <li>• By computer, group or user defined collections of computers</li> <li>• Automates the tedious process of researching, identifies which patches are installed and date installed, Monitors and maintains patch compliance for entire enterprise</li> </ul>
<b>Centralized Management of Patches</b>	<ul style="list-style-type: none"> <li>• Does not require multiple patch servers</li> <li>• Ensures that all systems are protected, even remote users on laptops and workstations</li> <li>• Allows implementation across entire network</li> <li>• Always know what patches and security holes reside on each user's system</li> </ul>
<b>Patch approval</b>	<ul style="list-style-type: none"> <li>• Approve or deny selected patches</li> <li>• Select by user defined computer collections</li> </ul>
<b>Automated patch deployment</b>	<ul style="list-style-type: none"> <li>• Schedule by time, computer, group or user defined collections of computers</li> <li>• Simultaneously deploy all required patches across operating systems</li> <li>• Single rollout strategy and policy enforcement</li> <li>• Maximize uptime</li> </ul>
	<ul style="list-style-type: none"> <li>• Select to deploy by patch or by computer</li> </ul>

ITEM	SPECIFICATION
<b>Interactive patch management</b>	<ul style="list-style-type: none"> <li>• Select individual computers, groups or user defined collections of computers</li> <li>• Ad-hoc simultaneous deployment of selected patches</li> <li>• Across operating systems</li> <li>• Across locations</li> </ul>
<b>Flexible configuration</b>	<ul style="list-style-type: none"> <li>• Patch file location, Patch file parameters</li> <li>• Reboot actions and notifications, By computer, group or user defined collections of computers</li> <li>• Saves bandwidth, Security and policy control</li> </ul>
<b>Comprehensive reports</b>	<ul style="list-style-type: none"> <li>• Graphical with drill-down, User defined</li> <li>• Scheduled, E-mail notification</li> <li>• Export to HTML, Excel or Word</li> </ul>
<b>SOFTWARE MANAGEMENT</b>	
	<ul style="list-style-type: none"> <li>• 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</li> <li>• Solution should be capable to create customized IT Procedures / Scripts or use pre-configured procedures</li> <li>• Solution should be able to support execution of CMD, Powershell, Batch File and VB Script</li> <li>• Solution should be able to easily deploy 3rd party applications</li> </ul>
<b>Cross-platform support</b>	<ul style="list-style-type: none"> <li>• Windows</li> <li>• MAC</li> </ul>
	<ul style="list-style-type: none"> <li>• Patches for 3rd party software is included, if made available by 3rd-party software package developers</li> </ul>
<b>Profile base policy</b>	<ul style="list-style-type: none"> <li>- Scan and Analysis</li> <li>- Override</li> <li>- 3rd-Party Software</li> <li>- Deployment</li> <li>- Alerting</li> </ul>
<b>Scan and Analysis</b>	<ul style="list-style-type: none"> <li>• Can Approve, Review and Reject Patch impact (Critical, Critical, Older than 30 days, Recommended, Virus Removal)</li> <li>• Schedule (Daily, Weekly, Monthly)</li> </ul>
<b>Override</b>	<ul style="list-style-type: none"> <li>• Can Approve/Reject Specific KB Override</li> <li>• Can Approve/Reject Specific MS Override</li> <li>• Can Approve/Reject Specific CVE, Product, or Vendor</li> </ul>
<b>3rd-Party Software</b>	<ul style="list-style-type: none"> <li>• Deploy popular 3rd-party software packages for both Windows and Apple operating systems</li> </ul>
	<ul style="list-style-type: none"> <li>• Reboot Options</li> </ul>



ITEM	SPECIFICATION
<b>Deployment</b>	<ul style="list-style-type: none"> <li>- Warn user and wait for x min and then reboot</li> <li>- Reboot immediately after update</li> <li>- Ask user about reboot and offer to delay</li> <li>- Ask permission, if no response in x min reboot</li> <li>- Skip reboot</li> <li>- Do not reboot after update, send email</li> </ul> <p><b>Procedures</b></p> <ul style="list-style-type: none"> <li>• Pre-Update Procedure</li> <li>• Pre-Reboot Procedure</li> <li>• Post-Update Procedure</li> <li>• Post-Reboot Procedure</li> </ul> <p><b>Schedule</b></p> <ul style="list-style-type: none"> <li>• Daily, Weekly, Monthly</li> </ul> <p><b>Blackout Window</b></p>
<b>Alerting</b>	<ul style="list-style-type: none"> <li>• New patch is available</li> <li>• Deployment fails</li> <li>• OS Auto Update changed</li> <li>• Create Alarm</li> <li>• Create Ticket</li> <li>• Email Recipients</li> <li>• Run a Procedure</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>• Dashboard</li> <li>• Patch Approval</li> <li>• Vulnerabilities List</li> <li>• Patch History</li> </ul>
<b>NON-INTRUSIVE REMOTE ACCESS</b>	
<b>General Features</b>	<ul style="list-style-type: none"> <li>• Solution should be capable of remoting a managed machine</li> <li>• 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</li> <li>• Solution should be able to record a remote session</li> <li>• Solution should be able to create multiple session of remote control</li> <li>• Solution should be able to access remote system without disturbing the user (background access)</li> <li>• Solution should be able to access the command prompt without disturbing the user</li> <li>• Solution should be able to access and modify the registry, services and processes without disturbing the user</li> <li>• Solution should be able to get audit information of the remote system without disturbing the user</li> </ul>

ITEM	SPECIFICATION
	<ul style="list-style-type: none"> <li>• Solution should be able to transfer, delete, copy file of the remote system without disturbing the user</li> </ul>
<p><b>Capability to access remote systems without disturbing the user</b></p>	<ul style="list-style-type: none"> <li>• Access to Command Prompt</li> <li>• Access to Event Viewer</li> <li>• Access to Asset Summary</li> <li>• Access to Registry</li> <li>• Access File Manager (Download, Rename, Delete, Move, Copy, Upload)</li> <li>• Access to Task manager</li> <li>• Access to Processes</li> <li>• Access to Services</li> <li>• Easy administration of users and policies</li> <li>• Access computers from anywhere</li> <li>• Password protected</li> </ul>
<b>REMOTE ACCESS</b>	
	<ul style="list-style-type: none"> <li>• Access computers from anywhere</li> <li>• Private Remote-Control Session for Windows</li> <li>• Shadow Support for Terminal Server Sessions</li> <li>• Remote Control Session is Logged</li> <li>• Supports Multiple Monitors</li> <li>• Supports Keyboard Mapping and Short-cut</li> <li>• Secure Communications</li> <li>• Peer to peer or relay connection</li> <li>• Provide the end user control and security to enable or disable remote control functions until granted approval</li> <li>• Screen Recording</li> </ul>
<b>TICKETING</b>	
	<ul style="list-style-type: none"> <li>• Accessible from a web browser</li> <li>• Automatically creates tickets based on alarm</li> <li>• Use email to update end users and receive feedback</li> <li>• Ticketing policies</li> <li>• Field customization</li> <li>• Clients can file tickets on their own</li> <li>• Auto assign tickets to technical personnel</li> <li>• Email notification of ticket status to client and technical personnel</li> <li>• Aging of tickets</li> </ul>
<b>REPORTING</b>	
	<ul style="list-style-type: none"> <li>• Detailed list, table and graphic style reports</li> <li>• Hardware and Software Inventory</li> <li>• Complete Computer Changes</li> </ul>

ITEM	SPECIFICATION
<b>Flexible Report Customization</b>	<ul style="list-style-type: none"> <li>• Disk Utilization</li> <li>• License Usage and Compliance</li> <li>• Network Usage and Statistics</li> <li>• Server and Workstation Uptime History</li> <li>• Help Desk Trouble Tickets</li> <li>• Computer Logs and Status</li> <li>• Schedule Reports for Automatic Distribution</li> <li>• Distribute automatically to selected e-mail recipients</li> </ul>
	<ul style="list-style-type: none"> <li>• Report for all, groups or specific computers</li> <li>• Detailed filtering and content selection</li> <li>• Add own logo</li> <li>• Immediate viewing with hyperlinks for quick data access</li> <li>• Save reports with selected parameters for reuse</li> <li>• Saved reports can be designated as private or shared</li> <li>• Export report data to HTML, Microsoft Word or Excel</li> </ul>
<b>ADMINISTRATION</b>	
<b>General Feature</b>	<ul style="list-style-type: none"> <li>• Solution should be able to limit the access to its module and visibility of machines per user</li> <li>• Solution should be able to be integrated to Windows Active Directory for solutions' login access</li> <li>• Solution should be able to specify its password strength and bad logon attempt policy</li> <li>• Solution should be able to propagate policies automatically without further user intervention once policies are assigned to machines, machine group or organization</li> <li>• Solution should be able to provide compliance reports of enforced securities and policies</li> </ul>
<b>Access Management</b>	<ul style="list-style-type: none"> <li>• Multi-tenant Capable</li> <li>• Ability to group systems</li> <li>• Assign Admin users</li> <li>• Ability to assign roles, scope and groups to Admin Users</li> <li>• Logs activities of Users using the system</li> <li>• Ability to access Admin system remotely</li> </ul>
<b>Centralized Management</b>	<ul style="list-style-type: none"> <li>• Ability to manage, monitor local and remote systems in a single console (without the need for a private connectivity).</li> <li>• Ability to deploy policies, monitoring definitions to both local and remote systems using a single console.</li> <li>• Ability to throttle bandwidth consumption used by agents and server to manage bandwidth and network traffic.</li> </ul>
<b>SECURITY</b>	

ITEM	SPECIFICATION
System Security	<ul style="list-style-type: none"> <li>• Compliance to HIPAA and PCI</li> <li>• Remote control sessions to end-user machines/servers is encrypted using Transport Layer Security (TLS)</li> <li>• Access to the user and admin web interface is encrypted using industry standard TLS</li> <li>• Agent will not accept any inbound connections, it is impossible for a third-party application to attack the agent from the network</li> <li>• All communication from the Agent originates from the agent outbound to the server.</li> <li>• Strong access control features (ability to control and manage machines is limited by both role and scope.</li> <li>• The Server combines passwords with unique randomly generated challenges for each attempt, hashed with SHA-256.</li> <li>• Protects against man-in-the-middle attacks by encrypting all communications between the agent and the server with FIPS certified 256-bit AES using a key that rolls every time the server task the agent, often multiple times per day.</li> <li>• There are no plain text data packers passing over the network.</li> <li>• Each time a technician remote administers, perform an action, or otherwise manages a system, it is logged in the system log.</li> <li>• Offers an optional system tray application which allows the end user to disable or enable remote control to the system.</li> </ul>
<b>SUPPORT</b>	
Competency	Provider should have at least 2 Certified Administrator of the Solution proposed.
Local Support	a) 1 year of updates and support b) 9 x 5 Phone, Onsite, E-mail and Chat support, One (1) hour response time upon receipt of call;

Prepared by:



**AMELITO V. DUCUT**  
 ITO III, COMD  
 Case Management Service