

## TERMS OF REFERENCE

### For the procurement of Desktop Management Solution

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.

### Desktop Management Software Technical Specifications:

LOT 1 : Desktop Management Software			
ITEM	QTY	UNIT COST	TOTAL
Desktop Management Software with Access License for 600 units	1 Lot	1,266,000.00	1,266,000.00
SUB TOTAL			₱ 1,266,000.00

### Unified Endpoint Management

The Management Tool must enable OSG to perform network management functions from one location using Single Console. A Management Suite that helps OSG to know about everything on our network by discovering and inventorying extensive management data about users and their managed or unmanaged devices. Manage mobile and desktop operating systems such as iOS, Android, Windows, Mac OS X, Linux, UNIX, and Chromebooks across highly distributed environments. OSG will gain one-click access to see, configure, and manage the IT policies and processes related to users and groups and all their associated devices. Actions are intelligent

and only take effect on the devices to which they apply. From a single console, you can distribute and update software or configuration settings, diagnose hardware and software issues, deploy OS images and migrate user profiles, perform vulnerability and patch management, use role-based administration to control user access to both features and devices, use remote control features to train end users or resolve problems, and more.

### **Role-based administration**

Management Suite that lets you manage console users with an extensive set of role-based administration features. OSG can:

- Assign granular feature-based group permissions
- Easily assign permissions to multiple users through local or LDAP user groups
- Synchronize console user configurations across multiple management servers

### **Single Management Console**

Must have Administrator console that lets you perform network management functions from one location. From a single console, you can distribute and update software or configuration settings, diagnose hardware and software issues, deploy OS images and migrate user profiles, use role-based administration to control user access to both features and devices, use remote control features to train end users or resolve problems, and more.

### **Single Agent**

Must employ a single agent for managed devices that provides wide range of configuration settings for various management feature such as inventory, remote control, software distribution, vulnerability and patch, software license monitoring. The single agent based will minimize the effort of deployment and management support.

### **Configurable Agent Settings**

The Agent configuration window lets you create new agent configurations for Windows, Linux, and Macintosh devices. The agent configurations you create can then be pushed to clients using the console's Scheduled tasks window.

### **Persistent Agent**

Agent Watcher is a tool that allows you to proactively monitor the status of selected agent services and files to ensure their integrity and preserve proper functioning on managed devices. Agent Watcher can be enabled and associated settings deployed with an initial device agent configuration. It can also be updated at any time without having to perform a full agent configuration. User must not be able to stop or remove the agent on their workstations without necessary privileges.

### **Agent Deployment**

OSG must be able to efficiently managed device and install the agent using the following method:

- MSI native support: Copy and paste MSI command line calls.
- Simplified bandwidth controls: Customize configurations appropriately.
- Task-based modeling: Separates package building and delivery task types to improve efficiency.
- Distribute large packages to multiple users with minimal bandwidth and without dedicated hardware or router reconfigurations.
- Allows you to access packages already delivered to a subnet.
- Installs prerequisite packages and enables you to automatically install multiple packages in a single operation.
- Task scheduler
- Integrates with directory-service and asset-inventory databases to help you easily select targets.
- Deploys any package type and provides access to multi-file MSI support.
- Provides Application self-service portal
- Deploys multiple software packages in a single policy and ensures the packages are available for future updating and reapplication if necessary

### **Remote Control**

The Management tool must provide a remote-control viewer to access a device. OSG requires the following features:

- Can only remote-control devices that have the remote-control agent installed.
- Requires user permission before remote control is started
- Provides alert to the user that their machine is being remote controlled.
- Support's remote view only
- Provides auditing of the remote session
- Able to define who can only perform remote control actions
- Remotely transfer files to and from your computer to another device.
- Remotely chat with a user at a remote device
- Remotely reboot a device.
- Able to define scope of machine that can only be controlled by specific roles or users
- Displays drawing tools you can use to draw on the remote screen if remote actions are not permitted

### **Platform Support**

A Desktop Management Solution must provide system management for Windows, Macintosh, Linux and Unix computers and devices. Provides wide range of support to Operating Systems

- Window Client
  - Mac OS X 10.6.8
  - Mac OS X 10.7.5
  - Mac OS X 10.8.5
  - Mac OS X 10.9.x
  - Mac OS X 10.10.x

- Mac OS X 10.11.x
- MacOS 10.12.x
- Windows XP Professional x32 SP3
- Windows XP Professional x64 SP2
- Windows Vista (32-bit) SP2 or higher
- Windows Vista (64-bit) SP2 or higher
- Windows 7 x32
- Windows 7 x64
- Windows 8 x32
- Windows 8 x64
- Windows 8.1 x64
- Windows 8.1 Update 1 x64
- Windows 10
- Windows 10 Anniversary Edition
- Windows 10 Creators Edition
- Windows Server
  - Windows Server 2003 Standard/Enterprise
  - Windows Server 2008 Standard/Enterprise
  - Windows Server 2012
  - Windows Server 2016 Standard
- Mobile Devices
  - Android
  - iOS
  - Blackberry OS1
  - Windows Mobile 6 or Higher1
  - Google Chromebook2

### **Monitoring and Alerting**

Alerting and monitoring must give OSG immediate notice of hardware, software, and application events on the devices being manage. When events occur that indicate a need for action or a potential problem, alerts initiate solutions by logging the event, sending an e-mail or pager message, running an application, or powering off the device.

The following general types of monitoring are available in Management Suite:

- Monitoring (pinging) devices for network connectivity
- Basic hardware and software monitoring for all devices
- Performance monitoring of selected hardware features
- Hardware-dependent monitoring using manufacturers' monitoring technology

### **OS Deployment and Provisioning**

Desktop Management Solution must support Operating System Provisioning. Following features are required: