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:

- The deployment of agent initiated centrally from the management server, and distributed via a push task.
- Distribution of agent via self-contained executable that is portable. This method will be more efficient and helps with many network configurations when network connectivity is a challenge
- Must have a deployment method that fully control the amount of bandwidth used during mas agent deployment.
- Other Operating System Support: Macintosh and Linux/Unix agents will work somewhat different than Windows based ones.

Auditing

Tool must have the auditing tool that audits console user activity and stores the auditing information in the core database and optionally the Windows event log.

Comprehensive Inventory

The inventory scanner collects hardware and software data and enters it into the core database. Desktop Management feature should include comprehensive inventory of assets. Required feature must contain these inventory-related features:

- Inventory scanning and inventory-related console features
- Custom data recording and retrieval
- Software Inventory
- Hardware Inventory including serial number of hardware
- Software license monitoring
- Unmanaged device discovery
- Reports for the above features

Reporting

The reporting tool can generate detailed reports that provide critical information about the devices on your network. This tool takes advantage of the Unified Management Solution inventory scanning utility, which collects and organizes hardware and software data, to produce useful, up-to-date reports.

Software Distribution

OSG requires the Management to have software distribution technology that helps IT staff implement controlled automation for fast and efficient software distribution and installation, security and virus update, and application patch management across mixed network environments. Should have a technology that is based on a modular, task-based model that can substantially improve overall efficiency in planning, scheduling and managing software distributions. Provides complete flexibility for packages, delivery task types, deployment scripts and target selection are managed separately to increase overall flexibility. OSG requires the following feature sets:

- Return code mapping: Defines return codes to improve application installation accuracy.

- Able to create provisioning templates including communications with users, moving all user profiles, laying down all supported and licensed applications, and standardizing your Windows and Mac OS X images.
- Use hardware-independent imaging to configure machines quickly with the appropriate drivers.
- Capture a profile from a previous OS, then deploy a new OS with the same profile, and previously installed software applications.
- Provisioning supports PXE booting and image deployment

Management Reporting and Dashboards

Management Tools must have business value dashboards that can be created in a brief timeframe and are ideal for executives among others to see and modify views into multiple sets of IT and business data.

Bandwidth Efficiency

OSG requires the management tool to have dynamic bandwidth throttling that specifies the network traffic a device has over distribution traffic. OSG requires the following features:

- Passive, low-bandwidth monitoring that the agent passively monitors product usage on devices, using minimal network bandwidth.
- Adjusts the priority of this specific task over other network traffic.

Software License Monitoring

Management tool must include Software license monitoring (SLM) that enables OSG to manage organization's software assets, such as tracking product usage, monitor license compliance, and ultimately control costs. OSG requires the following feature from Software License Management:

- Scan for known and unknown applications, define, and track previously unknown applications.
- Keep unauthorized software from running—even on computers not connected to the network and even if end-users rename the file.
- See comprehensive software license use with application usage, license reporting and compliance reporting.
- Able to deny application launch for specific groups of machines or users.

Managed Devices outside Corporate Network

Must be able to support managed devices outside the corporate network by using secure communication and functionality over the Internet. Must have the capability to perform remote installation, inventory, patching, and software distribution even if they are behind firewalls or use a proxy to access the Internet.

Reports and Data Analytics

Must be able to provide real time view of information using Data Analytics tools. This will significantly increase the IT asset management capabilities, in most areas of the business such as procurement, auditing, or inventory and security.

Support for Intel Vpro

Management tool must have Intel® vPro™ Support. OSG requires the following feature sets:

- Perform out-of-band discovery on Intel® vPro™-based hardware and software assets.
- Remotely heal Intel vPro-based systems regardless of OS or system state.
- Redirect screen output and use boot redirection to repair non-responsive systems.

Mobile Device Management

Desktop Management Solution must be able to enforce the highest level of security and compliance policies, without having to rely the device itself (which may be rogue), nor on a special-purpose container and duplicated collaboration applications (which may harm user experience). Mobile Device Manager must help OSG to take control of the mobile devices used in your company. It simplifies device provisioning, helps enforce corporate policies, and allows an administrator to lock or wipe lost or stolen devices. Mobility Manager adds these tools to the Management Suite console:

- **Android and iOS agents:** Allows you to manage Android and iOS devices, remotely lock, unlock, or wipe them, or configure device settings.
- **Mobile inventory:** An addition to your inventory that lists mobile devices that are under management or, if you set up the connection to an Exchange server, devices that have connected to your Exchange server.
- **Mobile software packages:** Distribute apps to mobile devices from a web server, or from the Google Play Store or Apple App Store.

Patch and Compliance

Desktop Management's Patch Management and Compliance must be complete, integrated security management that helps protect managed devices from a variety of prevalent security exposures and risks. Must have facility to use security scan tasks and policies to assess managed devices for known platform-specific vulnerabilities. Mus allow creation of custom definitions to scan for and remediate specific, potentially harmful conditions on devices. In addition to patch management, Patch and Compliance tool must perform the following tasks:

- Support for 3rd Party application patch
- Verify that the latest software is installed and up to date on your managed devices, as well as management servers and console machines.
- Use a blocked application definition to deny unauthorized or prohibited applications on devices.
- Use specific security threat definitions that detect the Windows firewall, turn it on or off, and configure the firewall settings.

- Patch and compliance for Macintosh devices
- Patch and compliance for Windows devices

Application Installation/Access On-Demand

Must provide a portal to end-user that delivers apps, documents, and links to end users so they can install items approved for use in OSG environment.

Power Management

Must have facility to monitor power usage on your managed computers from a central location. Should be able to create and deploy power management policies and generate reports to evaluate financial and power savings. OSG must be able to control the conditions under which computers and monitors stand by, hibernate, or power down. At the same time, must include a feature that lets users avoid specific power management actions (such as a hard shut down) using a client-side user interface.

Desktop Management Solution Checklist of Features:

High Level Functions
Discovery
Reporting & Dashboard
Inventory
OS Provisioning &Misgration
Power Management
Remote Control/Problem Resolution
Launch Pad
Software Distribution
Software Licensing Monitoring
Cloud Services Appliance or Management Gateway Appliance
Spyware Blocking/Removal
Patch Management
Application Blocking
Connection Control Manager
Host Intrusion Prevention
Antivirus Auditing
Audit & Compliance Enforcement
Role and Scope Based Administration
Supported Platforms Matrix
Client (Operating Systems)
Mac OS X 10.11.x
Mac OS 10.12.x
Windows 7 x32, x64
Windows 8 x32, x64

Windows 8.1 x64
Windows 8.1 Update 1 x64
Windows 10, Windows 10 Anniversary Edition, Windows 10 Creators Edition
Client (Server Operating Systems)
AIX 6.x x64 (PPC)
AIX 7.1 x64 (PPC)
CentOS 5 x32, x64
CentOS 6 x32, x64
CentOS 7 x64
HP-UX 11.31 PA RISC x64
11.31 on Itanium x64
Red Hat Enterprise Linux Advanced Platform 5 x32/x64
Red Hat Enterprise Linux 6 x32/x64
Red Hat Enterprise Linux 7 x64
Solaris 10 (SPARC64/ x86_64) with Update 8 or later
Solaris 11 (Sparcx64/ x86_64)
SuSE Linux Enterprise Server 11 x64
SuSE Linux Enterprise Server 12 x64
Windows Server 2008 Standard/Enterprise
Windows Server 2012
Windows Server 2016 Standard
Client (Embedded Operating System)
Windows Embedded 8.1
Client (Mobile Operating Systems)
Android
iOS
Google Chromebook
Console (Operating Systems)
Windows Server 2008 R2 Standard/Enterprise x64
Windows Server 2012 R2 Update 1 x64
Windows Server 2016
Windows 7 SP1
Windows 8 x64
Windows 8.1 Update 1
Windows 10
Core Server (Operating Systems)
Windows Server 2012 R2 Update 1 Standard x64
Windows Server 2016 x64
Core Server (Database)
MS SQL Server 2012
MS SQL Server 2012 Express
MS SQL Server 2014
MS SQL Server 2016

Systems Matrix
Queries/Directory manager
Active Directory (Import/Lookup)
LDAP
No schema extensions
User Management
Role-based administration
Managing authentications
Managing roles
Creating scopes
Create a team
Using remote control time restrictions
Inventory
Discover unmanaged devices
Collects hardware and software data
Adding software and data items
Custom data forms
Custom form builder
Add/remove software scanning
Actionable queries
Historical data
Rollup of multiple databases
Auditing
Configuring auditing
Sending auditing events to the Windows Event Viewer
Viewing auditing events
Creating filters for auditing event queries
Archiving and restoring auditing data
Reports
Canned reports
Custom reports
Customizable dashboards and portals
Remote Management
Remote control via LAN or WAN
Remote control via Internet
Remote control MAC
Send Ctrl-Alt-Del sequence
Auto lock (logoff) after session
Host blanking/KB and mouse lockout
Bandwidth control
Role based
Software Distribution

SW delivery to users
SW delivery to workstations
SW delivery over the Internet (no VPN)
Dynamic bandwidth throttling
Dynamic peer download
Multicast
Serverless load balancing, fault tolerance
Remote site Package Server option
Wake up, deliver app, shutdown
Chaining/task sequencing
Real-time Application launch denial
Application launch management
Package uninstall
MSI packaging tool
Bundle (msi, exe, actions, batch file, etc)
Windows and Batch file packages
Windows Script Host
PowerShell Scripts
Android & iOS Mobile
Power Management
Centralized control of power settings
Policy based
Variant scheme per hour/day
View current power settings
Remote shutdown
Automatic shutdown (after WOL+task)
Prompt before shutdown
Auto-protect data on shutdown
Defer shutdown if open application
Wake up with WOL standard
Wake up with Intel AMT standard
Wake up with internal system clock
Power modeling with custom wattage
Process termination (insomnia relief)
Critical process protection
Software Licensing Monitoring
Application-usage tracking
License-detail tracking
ISV data import
Reconcile PO, license, discovered SW
License downgrading
License compliance reports
Usage reports

Dynamic product definitions
Monitoring / Alerting
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
Send e-mail, page, snmp trap
Application Virtualization
No client requirement
No server requirement
Streaming
Virtualizes OS components (COM, IE, etc.)
App interconnectivity
User mode execution
License control
Usage monitoring
Run from removable media
Provisioning / OS Deployment
Windows imaging
Mac imaging
Linux imaging
Cloning (sector-based) option
PXE delivery
Remote imaging w/o dedicated HW
Driver management
Answer file management
ImageX support
3rd party image deployment
Profile migration
Hardware Independent Imaging
Multicast
Patch Management
Vulnerability assessment, remediation
Custom vulnerability definitions
Configuration baselining
Automatic remediation
Researched, pre-tested content
Process engine for automation
MS scan with OS, app content
RedHat, SUSE scan with OS, app content
MAC scan with OS, app content
Third-party application content
Third-party AV content, enforcement

Multicast
Dynamic peer download
Dynamic bandwidth throttling
CPU throttling for scanner
Defer during full-screen application usage
Assessment and remediation reports
Alerting by severity
Rollback/uninstall
Dark network patching
Endpoint Security
Host Intrusion Prevention System (HIPS)
Ivanti Firewall
Mobility Manager
Android and iOS agents
Mobile inventory
Mobile software packages
Intel vPro
Provisioning Intel vPro devices
Discovering vPro devices
vPro and the agent install
Intel vPro management features
LetMobile
Gateway-based BYOD security
Portal Manager
Delivers apps, documents, and links
Required policy-based
Cloud Services Appliance
Secure communication and functionality over the Internet
Configuring the core server to use a Cloud Services Appliance
Managing client certificates
Creating an on-demand remote control agent package