

## Service Description

---

### ProManage for Microsoft Endpoint Management

#### Introduction

Dell Technologies Services is pleased to provide ProManage for Microsoft Endpoint Management (the “Service(s)”) in accordance with this Service Description (“Service Description”). Your quote, or other mutually-agreed upon form of invoice or order acknowledgment will include the name of the service(s) and available service options that you purchased. For additional assistance or to request a copy of your service contract(s), contact technical support or your sales representative.

#### The Summary of Service

ProManage for Microsoft Endpoint Management provides comprehensive management of the Microsoft Endpoint Manager portfolio of services, including Microsoft Intune, Configuration Manager, Desktop Analytics, Co-management, and Windows Autopilot.

The ProManage for Microsoft Endpoint Management service delivers functions related to the day to day administration, ongoing support, optimization, and enhancements of the Microsoft Endpoint Management solution platform. This service is structured to provide the following:

- Management
- Maintenance
- Troubleshooting

ProManage for Microsoft Endpoint Management enables end user productivity and contributes to the security of end user devices. Dell Technologies Services works within ITIL-compliant processes to address issues as they occur, evaluate solution elements, and maintain the platform design to ensure optimal system performance for an existing implementation.

It is important to note that this management offer does not include licenses or procurement of licenses for Microsoft or other software, which are sold separately by Dell and other third parties. Additionally it is important to note there is a minimum seat count of 300 required for this offer.

#### Scope of Service:

ProManage for Microsoft Endpoint Management services are described in detail as follows:

##### **I. Microsoft Endpoint Management (MEM) Device Management**

Microsoft Endpoint Manager (MEM) covers both traditional legacy device management through use of System Center Configuration Manager (SCCM/ConfigMgr) as well as through modern mobile device

---

management (MDM) through Intune. Where SCCM requires specific Customer on-premise equipment and infrastructure, modern Intune MDM based management exists entirely through the cloud within Microsoft Azure, extending management to mobile device platforms like Android, iOS and iPadOS. Focus will be supporting a modern device management architecture utilizing Intune/MDM based management as preferred and wherever possible. Where required, hybrid-management utilizing SCCM will be performed, with focus on moving to a fully modern device management architecture utilizing Intune/MDM. The focus on modern management utilizing Intune/MDM ensures capitalizing on the investment of Azure (including M365 where applicable) and cloud-first based approach to endpoint management. This focus further enables a host of other capabilities based on Intune and Azure.

Dell Technologies Services will perform the following Microsoft Endpoint Management activities:

- **Windows 10 Management:** A comprehensive operating system lifecycle management across OEM's (Dell and non-Dell) devices, supporting desktop, laptop, and workstation (client) devices running any version of Windows 10 which is currently supported by Microsoft. Designed to support Customer owned (CO), bring your own (BYO), choose your own (CYO), and PC as a Service (PCaaS) scenarios. Windows 10 Management includes these components:
  - **Modern Provisioning Management:** Dell Technologies Services creates and manages Customer specific modern provisioning packages which are used to configure the Windows 10 operating system to Customer defined requirements. This process includes documenting Customer requirements, engineering the automation necessary to achieve the requirements, and quality testing the finished product.
  - **Windows as a Service:** Provides Customers with the fall release of the bi-annual Windows 10 feature releases (1x upgrade per year). This service leverages **Desktop Analytics** to assess the state of the Customers current application software and device driver environment. With this data, potential issues associated with the distribution of a Windows 10 feature release are identified, classified and remediated. Once any IT environmental remediation activities are complete, this service will package the Windows 10 feature release and engage the Operational Release Management (described below) service to distribute the update.
  - **Application Factory Services:** Creates customizable Windows installer based application packages for deployment to Windows 10 based devices. Each package is designed to install the desired application in the Customer's desired configuration. Customers will be able to select from a library of up to 30 most commonly used software titles, and have up to 5 custom application packages made available to them. The cost of any additional packages the Customer may require in a given year will be charged at the current factory rate.
- **iOS, iPadOS, & Android Management:** A comprehensive operating system lifecycle management, focused on the Customer's mobile platform. This Service will support all developer-supported versions of the iOS, iPadOS, or Google Android operating systems. iOS, iPadOS, & Android Management is also, designed to support Customer owned (CO), bring your own (BYO), choose your own (CYO), and Device as a Service (DaaS) scenarios.
  - **Mobile Device Management:** Dell Technologies Services will manage the Customer's mobile device population, including ensuring that user equipment is configured to a standard including a consistent set of applications and policies. This includes updating applications, patches and policies remotely with minimal impact to the Customer. Ensuring the platform and applications function correctly which includes troubleshooting and remote support. This also includes remote wiping and locking as required by the Customer. This may include implementing secure applications (email, access catalog etc.).
  - **Cross-platform Services:** Dell Technologies Services will support operational functions that apply across both in-scope Windows 10 and mobile device operating systems.
  - **Policy Management:** Dell Technologies Services will provide the Customer with engineered configuration policies while tracking where these policies are used and how these policies are

applied. Policy Management also provides Customers with proactive device certificate management services.

- **Operational Release Management (ORM):** Device management and maintenance enabling distribution of configuration changes to populations of end user computing devices. The ORM service delivers all functions related to the logistics, testing coordination, distribution, and distribution remediation of the following types of device changes:

- Application software and software updates
- Operating system quality and feature updates
- Configuration policies and scripts
- BIOS, firmware, and device driver updates

- **Windows Autopilot:** Dell Technologies Services will configure and maintain Windows Autopilot, enabling automated device provisioning using Autopilot's feature set to modernize the Customer's endpoint provisioning process. Autopilot for pre-provisioned deployment will enable deployment of fully provisioned devices directly to the end user. Autopilot Reset will enable rapid re-provisioning of existing assets to new users or secure retirement of devices that are being phased out of use.

- **Fine-Tuned User Experience:** Dell Technologies Services will use Microsoft Endpoint Analytics to monitor key areas such as startup, login, and software conflicts. These analytics are used to make proactive suggestions to increase the system performance. A measurement of the system is then converted to a numerical value so it can be compared to other systems in the fleet. This allows Dell Technologies Services to script proactive changes remotely or provide insight to the Customer.

- **Device Health:** Dell Technologies Services will manage the Microsoft Device Health as part of the defender security center. This includes monitoring storage, battery life, and time synchronization. These can be used to make suggestions about using the current hardware. In addition, Dell Technologies Services will also monitor application and drives on the systems and will potentially identify issue affecting the machine. Dell Technologies Services will attempt to repair issues remotely. If unsuccessful, Dell Technologies Services will bring the issue, and possible remediation, to the Customer's attention.

- **Microsoft OneDrive:** Dell Technologies Services will use OneDrive to supplement device provisioning as required to effectively manage the device.

- **Microsoft Power Automate:** Dell Technologies Services will support the Customer in setting up flows to automate functions of the service. Automations will be operational in nature and increase efficiency of the Customer's device management.

- **Microsoft Power BI Pro:** Dell Technologies Services will provide standard reporting and dashboards to the Customer using MS Power BI Pro, providing detailed data about the Customer's device management.

- **Azure Active Directory Premium 1 (P1):** Dell Technologies Services will join the Customer's devices to Azure Active Directory domain (AAD) leveraging these features:

- **Device Registration (Azure AD):** Dell Technologies Services will add devices to access Customer Azure AD as determined by the Customer. This service will be managed under Customer direction. This may include enforcing policies such as roaming, Single sign-on (SSO) and, access and password reset in sections of the remote system.
- **Azure AD Domain Join:** Dell Technologies Services will add and remove devices to Customer Azure AD (if applicable) for the purpose of device provisioning. This will include setting up scripts for use of OOBE, autopilot and remote tools. This will include troubleshooting issues around these functions and maintaining the knowledgebase for other services.

## II. Service Interface Guide for ITSM Tools

Dell Technologies Services will coordinate and comply with secure methods and information security policies to ensure the highest integrity in the protection of information.

Dell Technologies Services will provide tier 2 support for system administrators and named stakeholders. Support is delivered via direct engagement with the Service Engineer.

## **Management**

### **Incident/Problem Management**

Dell Technologies Services will customize the MEM incident / problem management process to complement existing established ITIL processes. This process can be initiated in two ways; 1) an alert event is generated by an existing infrastructure monitoring application, or 2) an incident/ problem is sent to the established MEM infrastructure team via email.

### **Change Management**

Dell Technologies Services will utilize the Customer's existing Change Management process.

### **Solution Platform Design Management**

As business needs and the features of MEM evolve, alterations to the design of the solution may also be necessary to continue to meet the needs of the organization. Dell Technologies Services accommodates these situations by engaging with Customer stakeholders, either on a planned annual or an as needed basis, to review potential changes to requirements and propose design updates to meet the new requirements of the infrastructure. If the Customer approves the new design and acquires the requisite hardware and/or software components, Dell Technologies Services will work to implement the new design. The implementation process will identify each task and create a timeline for the completion of each task. Dell Technologies Services will then draft a rollback plan and submit the changes for review and approval as per the established change management process. Large and/or complicated implementations involving other infrastructure elements may require formal project management services which are not included with this service.

## **Maintenance**

The maintenance aspects of the Microsoft Endpoint Management service follow closely the manufacturer's best practice recommendations for keeping the solution platform operating optimally. The solution platform maintenance activities are broken down by period as follows:

### **Daily Tasks**

- Review alerts generated by established monitoring application
- Validate the availability of the MEM solution platform and related services
- Evaluate MEM tool and device end point health status
- Monitor the platform message queue and associated inbox
- Validate distribution point replication
- Review platform for long running queries or stalled activities
- Review audit messages for actionable events

### **Weekly Tasks**

- Remove obsolete objects & files from site systems
- Check advertisement & package status

- Review sync between solution components and related distribution points

### Monthly Tasks

- Validate database maintenance & stale object deletion performed by DB Admins
- Assess advertisement success/ failure rate
- Review platform updates for all solution components
- Execute performance review & tuning

### Quarterly Tasks

- Conduct package & distribution collection archival

### Annual Tasks

- Review MEM design & capacity planning
- Review & update solution platform documentation

## Troubleshooting

In addition to direct troubleshooting and remediation of MEM and its components through the incident / problem management process, Dell Technologies Services will require collaboration with additional support stakeholders to ensure the optimal operation of other enterprise components which may affect MEM. This collaboration shall be limited as follows:

- Working with Server Administrators to ensure that the Windows server operating system is properly configured and managed to support the MEM component(s)
- Engaging with Active Directory and Azure Active Directory administrators for troubleshooting issues related to the configuration and synchronization of their directories
- Working with SQL database administrators to ensure the requisite database is available to the solution platform and that it complies with Microsoft's configuration guidance
- Collaborate with network teams to ensure that communications ports and protocols are allowed between MEM infrastructure components as per Microsoft's requirements
- Participate as requested in day-to-day operational activities with other Dell Technologies Services resources to facilitate the best practice operation of MEM

## III. Microsoft Endpoint Management Security

Dell Technologies Services will perform the following as part of Microsoft Endpoint Management Security:

- **Remote access to applications**
  - Connect Customer's on-premises infrastructure to the Microsoft cloud, in order to enable Customer access to on-premises web applications.
- **Device and Application Management**
  - Remotely provision and deploy new Customer devices with Windows Autopilot
  - Leverage Windows Defender to detect and protect against threats
- **Resource Protection**
  - Discover cloud applications and services used in the Customer's organization
  - Onboard Customer machines to Microsoft Defender ATP
- **Threat Protection**

- **Windows Defender Antivirus:** Configure and manage the software via MEM, Group Policy, WMI, or Intune. Dell Technologies Services will update policies to ensure proper device protection and enrollment
- **Microsoft Defender Advanced Threat Protection:** Configure and manage the software via MEM, Group Policy, WMI, or Intune. Dell Technologies Services will update policies to ensure proper device protection and enrollment. Dell Technologies Services will monitor devices for threats and provide the following:
  - Report alerts to the Customer
  - Provide specific details on action to be taken
  - Block, quarantine, or auto-remediate based on rules configured in the console
  - Consult with the Customer on the issue and determine next steps
  - Invoke next steps based on Customer's incident response plan as needed
  - Notify Customer of alerts on potentially unwanted programs to determine if it's safe or needs to be removed from the environment
  - Update safelist for programs periodically
  - Advise on vulnerability management for programs that have known vulnerabilities and/or need patched due to age
- **Exploit Protection:** Configure and manage exploit protection to ensure proper device protection. Run in audit mode as issues arise to not disrupt end users.
- **Controlled Folder Access:** Configure and manage controlled folder access. Audit mode will be applied for testing behavior before rollout.
- **Device Control:** Configure and manage device control for USB devices to include:
  - Microsoft Defender Antivirus real-time protection (RTP) to scan removable storage for malware.
  - The Attack Surface Reduction (ASR) USB rule to block untrusted and unsigned processes that run from USB.
  - Direct Memory Access (DMA) protection settings to mitigate DMA attacks, including Kernel DMA Protection for Thunderbolt and blocking DMA until a user signs in.
- **Web Protection:** Setup and configure web protection and content filter based on Customer input. Sites and traffic can be blocked based on preference, category, or content. Dell Technologies Services will investigate alerts on traffic periodically that may flag an alarm for the Customer and report on this to determine if the traffic is abnormal.
- **Information Protection**
  - **Bitlocker:** Dell Technologies Services will set up and manage the Customer Bitlocker environment using AES 256 encryption. Dell Technologies Services will suggest actions based on Microsoft Power BI Pro compliance reporting. Dell Technologies Services will help manage the emergency keys and provide an automated unlocking system. Dell Technologies Services will help with trouble shooting Bitlocker issues.
- **Identity and Access Management**
  - **Multi-factor Authentication (2fA):** Assist Customer with security policy and configuration of multi-factor authentication including:
    - Policy Setup

- Security configuration
- Feature overview for ADFS, smart lockout, and self-service password reset
- **Conditional Access:** Configure and deploy conditional access based on Customer policy and security decision settings. Dell Technologies Services will assist with scenario creation for applying conditional access:
  - Requiring multi-factor authentication for users with administrative roles
  - Requiring multi-factor authentication for Azure management tasks
  - Blocking sign-ins for users attempting to use legacy authentication protocols
  - Requiring trusted locations for Azure Multi-Factor Authentication registration
  - Blocking or granting access from specific locations
  - Blocking risky sign-in behaviors
  - Requiring organization-managed devices for specific applications

## Deliverables

The following is a list of tangible material provided as part of the Service:

- Monthly performance reports described in this document
- Monthly invoice based on Microsoft licensed user count

## Assumptions

Dell Technologies Services has made the following specific assumptions while specifying the Services detailed in this Service Description:

- Customer owns, or will procure upon contracting, the Enterprise Mobility + Security (EMS) and Azure Premium 1 (P1) license bundles from a Microsoft CSP partner. Other Microsoft license bundles that contain these components are also acceptable.
- Customer's end user devices are all running Windows 10 or newer Microsoft operating systems
- Customer must designate Dell as the Claiming Partner of Record (CPOR) with Microsoft

## Exclusions

For the avoidance of doubt, the following activities are not included in the scope of this Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The Service does not include the development of any intellectual property created solely and specifically for the Customer, as defined below.
- Cost of consumables, replacement parts, hardware, software, network upgrades and associated services.
- Except as otherwise stated in this Service Description all server, network device and software upgrades.
- Manufacturer warranty parts, labor, and services.
- Customer printers (whether stand-alone or network attached).
- Any non-support or administrative-oriented activities such as technical projects, including but not limited to, PC deployments, hardware upgrades, and software installations.

- File restoration and data backup.
- Problems occurring in applications or devices not listed on the agreed upon Inventory.
- Mass setup of new devices, PCs or peripherals.
- Certain third-party or custom application support, unless mutually agreed by Dell Technologies Services and Customer during the on-boarding process.
- In the event an endpoint is too old or is being used for tasks that are greater than the endpoint was designed for, Dell Technologies Services reserves the right to remove such items from the Service.
- Although Dell Technologies Services will design a remediation plan, any actual remediation work, if performed, will be subject to a separately signed services engagement subject to additional fees.
- Dell Management of Windows systems running operating systems older than Windows 10.
- Dell Management of MacOS.
- Mobile Device Management does not include physical device repair or replacement and it does not include provider plan management.
- Microsoft Power Automate: Dell Technologies Services will not provide integration services with external tool sets or build flows not used by Dell.
- Microsoft Power BI Pro: Dell Technologies Services will not provide integration services with external tool sets or build reports not used by Dell.
- Device Registration (Azure AD): Does not include resolving issues on the non-corporate part of the OS that are due to the use of unapproved software.
- Azure AD Domain Join: Does not include managing Azure AD, on prem AD, or interface issues.
- Device Control: Dell Technologies Services will not configure code integrity.
- Bitlocker: Dell Technologies Services will not manage keys over 4 years old or an on-premise Microsoft BitLocker Administration and Monitoring System (MBAM).

Dell Technologies will also escalate all out of scope and unsupported technologies directly to the Customer's designated point of contact (POC) or a third-party. Escalation will include notification of the issue, steps taken to date, transfer of incident ownership, and contact information to provide updates.

This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of your master services agreement or Agreement, as defined below, as applicable.

### Offer-Specific Customer Responsibilities

- Knowledgeable Customer representative(s) must actively cooperate with Dell ProManage staff while onboarding the Customer. Required cooperation may include, but is not limited to, providing user identities.
- Register Dell Technologies as the Claim Partner of Record with Microsoft.
- Provision the base hardware warranty entitlement for all enrolled endpoint devices throughout the life of the Managed Services engagement with Dell Technologies Services.
- Maintain an active Dell ProSupport entitlement on all Dell enrolled endpoint devices throughout the life of the ProManage services engagement with Dell Technologies Services.
- Designate a single, knowledgeable and authorized point of contact (POC) who will serve as the primary interface between the Customer and the Dell ProManage Experience Manager, and have the appropriate authority to request and modify services. Additionally, the Customer must provide a named Customer IT Admin point of contact POC. The Customer may also designate additional representatives to request services as deemed appropriate.
- Allow Dell Technologies Services to install "agents" onto enrolled endpoint device. Dell Technologies Services utilizes an automated software agent, which will be installed and configured to ensure critical and regular maintenance on each system is routinely performed. Installed "agents" shall be allowed to report telemetry back to Dell.



- The Customer agrees to provide high-speed Internet connection to be used for remote access into the Customer's network, including access and administrative credentials (i.e., usernames and passwords) to Customer's devices.
- Customer provides Dell with provision access to Customer environment, including direct access to the new or existing M365 tenant.
- Customer must agree to a single bill across all locations (within the same region)
- Customers with multiple domains (i.e. multiple forests or stand-alone domains), will require a single AD/bind account, that can query all domains enrolled for user authentication and verification.
- For any/all (e-mail) domains Customer wishes to register for enrollment, it must be possible to send an e-mail with a registration link, that Customer can receive and accept
- Controlled Folder Access: Customer must supply the applications and root directories that are needed to configure for proper access control.

## General Customer Responsibilities

**Authority to Grant Access.** Customer represents and warrants that it has obtained permission for both Customer and Dell Technologies Services to access and use, whether remotely or in-person, Customer-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing these Services. If Customer does not already have that permission, it is Customer's responsibility to obtain it, at Customer's expense, before Customer asks Dell Technologies Services to perform these Services.

**Non-solicitation.** Where allowed by law, Customer will not, without Dell Technologies Services' prior written consent, for a period of two years from the date listed on your Order Form, directly or indirectly solicit for employment any Dell Technologies Services employee with whom you have come in contact in connection with Dell Technologies Services' performance of the Service; provided, however, that general advertisements and other similarly broad forms of solicitation will not constitute direct or indirect solicitation hereunder and you are permitted to solicit for employment any employee that has been terminated or has resigned his or her employment with Dell Technologies Services prior to the commencement of employment discussions with you.

**Customer Cooperation.** Customer understands that without prompt and adequate cooperation, Dell Technologies Services will not be able to perform the Service or, if performed, the Service may be materially altered or delayed. Accordingly, Customer will promptly and reasonably provide Dell Technologies Services with all cooperation necessary for Dell Technologies Services to perform the Service. If Customer does not provide reasonably adequate cooperation in accordance with the foregoing, Dell Technologies Services will not be responsible for any failure to perform the Service and Customer will not be entitled to a refund.

**On-site Obligations.** Where Services require on-site performance, Customer will provide (at no cost to Dell Technologies Services) free, safe and sufficient access to Customer's facilities and environment, including ample working space, electricity, safety equipment (if applicable) and a local telephone line. A monitor or display, a mouse (or pointing device), and a keyboard must also be provided (at no cost to Dell Technologies Services), if the system does not already include these items.

**Data Backup.** Customer will complete a backup of all existing data, software and programs on all affected systems prior to and during the delivery of this Service. Customer should make regular backup copies of the data stored on all affected systems as a precaution against possible failures, alterations, or loss of data. Dell Technologies Services will not be responsible for the restoration or reinstallation of any programs or data.

Unless otherwise required by applicable local laws, DELL TECHNOLOGIES SERVICES WILL HAVE NO LIABILITY FOR:

- ANY OF YOUR CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION;

- LOST OR CORRUPTED DATA, PROGRAMS OR SOFTWARE;
- DAMAGED OR LOST REMOVABLE MEDIA;
- THE LOSS OF USE OF A SYSTEM OR NETWORK; AND/OR
- FOR ANY ACTS OR OMISSIONS, INCLUDING NEGLIGENCE, BY DELL TECHNOLOGIES SERVICES OR A THIRD-PARTY SERVICE PROVIDER.

**Third Party Warranties.** These Services may require Dell Technologies Services to access hardware or software that is not manufactured or sold by Dell Technologies Services. Some manufacturers' warranties may become void if Dell Technologies Services or anyone else other than the manufacturer works on the hardware or software. Customer will ensure that Dell Technologies Services' performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Customer. Dell Technologies Services does not take responsibility for third party warranties or for any effect that the Services may have on those warranties.

**Service Hours.** Subject to local law relating to weekly work hours, unless otherwise listed below, this Service will be performed Monday through Friday during normal Dell Technologies Services business hours, which is from 8:00 AM to 5:00 PM Customer Local time:

No Service activities will take place outside normal business hours or during local holidays unless other arrangements have been made in advance in writing.

## Services Terms & Conditions

This Service Description is entered between you, the Customer (“you” or “Customer”), and the legal entity identified on your Order Form for the purchase of this Service (the “Dell Legal Entity”). This Service is provided subject to and governed by Customer’s separate signed master services agreement with the Dell Legal Entity that explicitly authorizes the sale of this Service. In the absence of such agreement, depending on Customer’s location, this Service is provided subject to and governed by either Dell’s Commercial Terms of Sale or the agreement referenced in the table below (as applicable, the “Agreement”). Please see the table below which lists the URL applicable to your Customer location where your Agreement can be located. The parties acknowledge having read and agree to be bound by such online terms.

Customer Location	Terms & Conditions Applicable to Your Purchase of the Services	
	Customers Purchasing Services Directly	Customers Purchasing Services Through an Authorized Reseller
United States	<a href="https://www.dell.com/CTS">Dell.com/CTS</a>	<a href="https://www.dell.com/CTS">Dell.com/CTS</a>
Canada	<a href="https://www.dell.ca/terms">Dell.ca/terms</a> (English) <a href="https://www.dell.ca/conditions">Dell.ca/conditions</a> (French-Canadian)	<a href="https://www.dell.ca/terms">Dell.ca/terms</a> (English) <a href="https://www.dell.ca/conditions">Dell.ca/conditions</a> (French-Canadian)

\* Customers may access their local [Dell.com](https://www.dell.com) website by simply accessing [Dell.com](https://www.dell.com) from a computer connected to the Internet within their locality or by choosing among the options at Dell’s “Choose a Region/Country” website available at [Dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen](https://www.dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen).

Customer further agrees that by renewing, modifying, extending or continuing to utilize the Service beyond the initial term, the Service will be subject to the then-current Service Description available for review at [Dell.com/servicesdescriptions](https://www.dell.com/servicesdescriptions).

If there is a conflict between the terms of any of the documents that comprise this Agreement, the documents will prevail in the following order: (i) this Service Description; (ii) the Agreement; (iii) the Order Form. Prevailing terms will be construed as narrowly as possible to resolve the conflict while preserving as much of the non-conflicting terms as possible, including preserving non-conflicting provisions within the same paragraph, section or sub-section.

By placing your order for the Services, receiving delivery of the Services, utilizing the Services or associated software or by clicking/checking the “I Agree” button or box or similar on the Dell.com website in connection with your purchase or within a Dell software or Internet interface, you agree to be bound by this Service Description and the agreements incorporated by reference herein. If you are entering this Service Description on behalf of a company or other legal entity, you represent that you have authority to bind such entity to this Service Description, in which case “you” or “Customer” shall refer to such entity. In addition to receiving this Service Description, Customers in certain countries may also be required to execute a signed Order Form.

## Supplemental Terms & Conditions

**1. Term of Service.** This Service Description commences on the date listed on your Order Form and continues through the term (“**Term**”) indicated on the Order Form. As applicable, the number of systems, licenses, installations, deployments, managed end points or end-users for which Customer has purchased any one or more Services, the rate or price, and the applicable Term for each Service is indicated on Customer’s Order Form. Unless otherwise agreed in writing between Dell Technologies Services and Customer, purchases of Services under this Service Description must be solely for Customer’s own internal use and not for resale or service bureau purposes.

## 2. Important Additional Information

- A. **Rescheduling.** Once this Service has been scheduled, any changes to the schedule must occur at least 8 calendar days prior to the scheduled date. If Customer reschedules this service within 7 days or less prior to the scheduled date, there will be a rescheduling fee not to exceed 25% of the price for the Services. Any rescheduling of the Service will be confirmed by Customer at least 8 days prior to commencement of the Service.
- B. **Payment for Hardware Purchased With Services.** Unless otherwise agreed to in writing, payment for hardware shall in no case be contingent upon performance or delivery of services purchased with such hardware.
- C. **Commercially Reasonable Limits to Scope of Service.** Dell Technologies Services may refuse to provide Service if, in its commercially reasonable opinion, providing the Service creates an unreasonable risk to Dell Technologies Services or Dell Technologies Services' Service providers or if any requested service is beyond the scope of Service. Dell Technologies Services is not liable for any failure or delay in performance due to any cause beyond its control, including Customer's failure to comply with its obligations under this Service Description.
- D. **Optional Services.** Optional services (including point-of-need support, installation, consulting, managed, professional, support or training services) may be available for purchase from Dell Technologies Services and will vary by Customer location. Optional services may require a separate agreement with Dell Technologies Services. In the absence of such agreement, optional services are provided pursuant to this Service Description.
- E. **Assignment and Subcontracting.** Dell Technologies Services may subcontract this Service and/or assign this Service Description to qualified third party service providers who will perform the Service on Dell Technologies Services' behalf.
- F. **Cancellation.** Dell Technologies Services may cancel this Service at any time during the Term for any of the following reasons:
- Customer fails to pay the total price for this Service in accordance with the invoice terms;
  - Customer is abusive, threatening, or refuses to cooperate with the assisting analyst or on-site technician; or
  - Customer fails to abide by all of the terms and conditions set forth in this Service Description.

If Dell Technologies Services cancels this Service, Dell Technologies Services will send Customer written notice of cancellation at the address indicated on Customer's invoice. The notice will include the reason for cancellation and the effective date of cancellation, which will be not less than ten (10) days from the date Dell Technologies Services sends notice of cancellation to Customer, unless local law requires other cancellation provisions that may not be varied by agreement. If Dell Technologies Services cancels this Service pursuant to this paragraph, Customer shall not be entitled to any refund of fees paid or due to Dell Technologies Services.

- G. **Geographic Limitations and Relocation.** This Service is not available at all locations. Service options, including service levels, technical support hours, and on-site response times will vary by geography and certain options may not be available for purchase in Customer's location, so please contact your sales representative for these details.

© 2017 Dell Inc. All rights reserved. Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. A printed hardcopy of Dell's terms and conditions of sale is also available upon request.