DELL Technologies

Service Description

Managed Detection and Response with Microsoft

Introduction

Dell Technologies Services is pleased to provide Managed Detection and Response with Microsoft Service (the "Service(s)") in accordance with this Service Description ("Service Description"). Your quote, order form or other mutually-agreed upon form of invoice or order acknowledgment (as applicable, the "Order Form") 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 Scope of This Service

The Service seeks to provide the Customer with Managed Detection and Response with Microsoft Services.

The Service is provided remotely. The Customer is responsible for all Microsoft licensing and subscriptions; **Microsoft licenses are not included as part of this Service.** Please refer to the **Technical Data Sheet** for details regarding the Customer data volume limits under this Service.

Key components of the Service are described in table 1 below:

Table: 1

Service purchased	Key components of the Service
Managed Detection and Response with Microsoft	• Services leveraging technology from Microsoft Defender XDR and Microsoft Sentinel for the management platform. • Operating hours: 24 hours a day, 7 days a week (24x7) • Service Kickoff/Initiation • Tenant Enablement & Readiness • Onboarding • Detection • Threat Response • Service-related Security Configuration • Quarterly Reporting • Incident Response

	• Includes above components, leveraging Customer currently licensed XDR account. • Customers purchasing the Service-only offer must meet the minimum software module requirements to receive Services.

Note: The product capability is dependent on the Microsoft licensing / subscription that Customer has purchased to protect Customer workloads; this will impact the Dell Technologies Services team's available remediation options.

Operating hours

The Dell Technologies Services virtual security operation centers (SOC) are designed to provide customer with a 24 hours a day, 7 days a week (24x7) service.

The Service provides a complete solution to a Customer's IT environment, providing security to devices, network, user activity, cloud applications and cloud resources, leveraging technology from Microsoft Defender and Sentinel as the management platform.

The Service includes monitoring of these Microsoft components through Microsoft Sentinel as part of the baseline offering:

M365 Defender Products in Scope for Monitoring:

Microsoft Defender for Office 365

Microsoft Defender for Endpoint (minimum required service)

Microsoft Defender for Servers (onboarded to Microsoft Defender for Endpoint)

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Pre-requisites needed for Case Management/Monitoring

Microsoft Sentinel (minimum required service)

Note: A dedicated Azure Subscription and Workspace is required for the Service.

Tenant Enablement & Readiness Services are provided during normal business hours. Tenant Enablement & Readiness must be completed prior to a customer being onboarded into Dell's 24/7 managed SOC.

Table 2 below lists each of the Elements of the Key components of the Service.

Table: 2

Key Component	Elements
Service Kickoff/Initiation	• Service initiation meeting (kickoff meeting) • Create Customer Account in ITSM platform • Customer completed pre-engagement checklist
Tenant Enablement & Readiness	• License and Subscription Pre-Requisite review • Pre-deployment Planning • Defender Policy Review/Configuration • Connectors and Data Sources

	• Data Ingestion and Log Collection • MDR Monitoring and Reporting
SOC Onboarding	• Review Customer IT Environment • Service enablement
Detection	• 24x7 Access to security analysts • Threat detection and investigations • Dell initiated Threat Hunting
Threat Response and Security Configuration	• Threat Response • Service-related Security Configuration • Remote Remediation related to the incident
Quarterly Reporting	• Quarterly Report • Security recommendations
Incident Response	• Remote Incident Response initiation
Project Management	• Manage delivery of this engagement

Detailed Description

Service Kickoff/Initiation:

Service initiation meeting
A Dell Technologies Services Project Manager will call for a meeting to review Service expectations and requirements with Customer in order to plan delivery of the Service. Goal of the Service initiation meeting is to:

- Review and discuss Customer profile responses to understand Customer's IT environment, security controls, and any other relevant context.
- Provide guidance on current detection mechanisms in the Customer environment and how they can be applied to the Customer.
- Provide guidance on Service integrations with third-party software and hardware.

Should the Customer have additional requirements outside the scope of this Service Description, assistance with these requirements would be proposed as an additional service for an additional fee.

Customer completed pre-engagement checklist
Customer is responsible for completing the pre-engagement checklist prior to the IT environment review. The pre-engagement checklist is sent by the Dell Technologies Services project manager and contains a detailed checklist and IT environment specifications.

Review of IT Environment
The IT environment review is an activity performed to gather data about Customer's existing IT environment into which the Service will be implemented.

Tenant Enablement & Readiness

Dell Technologies Services will provide guidance on core components to support the Service. Tenant Enablement & Readiness is designed to make sure the Customer's IT environment meets the minimal required configurations to provide 24/7 monitoring.

Based on initial review of the Customer's IT environment, Dell Technologies Services will provide guidance to Customer in the configuration of Defender baseline policies and configuration of the (if required) Sentinel workspace.

Please refer to the **Technical Data Sheet** for additional details regarding the limits of Tenant Enablement & Readiness under this Service.

Overview of Tenant Enablement & Readiness

1) Licensing and Subscription**:** ensure the Customer has the necessary licenses and subscriptions for Microsoft 365 Defender. Identify need for additional Customer licenses, based on the Customer's organizational needs.

2) Pre-deployment Planning**:** review the Customer's security needs and existing infrastructure.

3) Defender Policy Review/Configuration**:** activate Microsoft 365 Defender components within Customer's Microsoft 365 admin portal, as needed. With the Customer's approval, assist with the configuration of baseline security settings within the Defender portal(s).

4) Data Connectors, Data Ingestion, and Log Collection**:** integrate Microsoft 365 Defender with Customer's Sentinel environment to centralize security event logs and alerts, when available and only as directed by Customer. Advise on the implementation of supported data connectors to collect security data from Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft Defender for Identity.

5) MDR Monitoring and Reporting**:** enable transition to continuous monitoring of the security status of Customer's IT environment using the Microsoft Defender Security Center.

SOC Onboarding

Service enablement:

- Verify tenancy prerequisites for the Service
- Guide Customer through the process of provisioning access to the Dell Technologies Services team
- Guide Customer through Role-Based Access Controls (RBAC) Assignments required for M365 Defender XDR access

  Note: The above activity is applicable only if Microsoft Sentinel / Microsoft Defender for Servers (Microsoft Defender for Cloud) is in scope.
- Guide Customer through Microsoft Sentinel and Azure Lighthouse configuration
- Guide Customer through Microsoft Sentinel and Azure Lighthouse configuration for Microsoft Sentinel / Defender for Cloud ARM template for Defender for Servers management
- Set up Basic Automation Rule / Playbook for Customer response on a security Incident and any SOC required automation

- Investigation and Case Management is documented via the Customer's Microsoft Sentinel/Defender instance in conjunction with Dell's ServiceNow/ITSM instance. Dell Technologies Services will work with the Customer to configure this capability. Any Customer request or queries related to an incident or the Services, should be raised via the ServiceNow/ITSM platform.

Detection

Transition to Steady State:

Dell Technologies Services' recommendation is to onboard Customer's Defender and Sentinel tenant as expediently as possible, ideally within a month of Services start (not recommended beyond that), which maximizes the insights and monitoring that the Service provides.

Real-time and historic data (subject to Microsoft products capabilities and storage settings):

- Relevant security events determined by Dell Technologies Services to be "true positives" and requiring Customer action will be escalated to Customer within the service levels detailed below
- Events determined to be "false positive" or automatically remediated will be noted in the Customer's quarterly report
- Custom indicators of compromise provided by Dell Technologies Services will be analyzed as they are received or created

24x7 Access to Security Analysts
Dell Technologies Services security analysts are available on a 24x7 basis to assist with relevant inquiries.

Threat Detection and Investigations
Review and investigate threats detected within the XDR application. Threats requiring further analysis as determined by Dell Technologies will result in the creation of an Investigation within the Microsoft Defender XDR and Sentinel applications. Dell Technologies will contact Customer through the XDR portal, email, or supported integrations if sufficient evidence is collected to deem a threat as malicious, or if Dell Technologies requires further input from Customer to proceed with the Investigation.

Threat Hunting
Dell Technologies conducts Threat Hunting across the Customer's IT environment for relevant indicators of compromise and tactics collected from current Incident Response engagements. Threat Hunting activities are limited to data gathered through the XDR platform. Dell Technologies will inspect collected Customer telemetry to detect activity such as the presence of persistence mechanisms, anomalous user activity, threat actor tactics, anomalous network communications, and anomalous application usage. Threats detected as part of the Threat Hunting process will result in creation of an investigation and notification to Customer through the XDR portal, email, or supported integrations.

Threat Response

During onboarding, Customer will pre-approve select Threat Response actions which may be taken as part of the Service. Dell Technologies Services will perform Threat Response actions leveraging the XDR platform.

Service-related Security Configuration

Dell Technologies Services may approve up to 40 hours of remote, Service-related Security Configuration as needed to assist Customer for each quarter in the Term of Service. Security Configuration is specifically limited to investigations and/or alerts resulting from provision of the Service, and may include:

- MDR endpoint agent troubleshooting and best practice guidance.
- Guidance with updates to XDR platform policies.
- Guidance configuring and integrating third-party on applications into the XDR platform.

Should more than 40 hours of service-related Threat Response and Security Configuration assistance be required in a single quarter during the Term of Service, Customer can work with their Dell Technologies account manager to purchase additional time. Any unused time at the end of each quarter of the Term of Service will be forfeited. Additional time purchased for a future quarter within the Term of Service cannot be used before the start of the quarter for which it was purchased.

Quarterly Reporting

Dell Technologies Services will provide quarterly reporting on trends and notable activity observed within Customer's IT environment through Service platform, and provide recommendations on how to defend against threats. The Quarterly Report includes a review of investigations and alert trends, analytics, and security posture guidance.

Incident Response

Upon notification by the Dell Technologies Services security analyst, the following remote Incident Response components are available.

Remote Incident Response Initiation

Dell Technologies Services will provide up to 40 hours of remote Incident Response assistance to Customer for each **year** during the Term of Service, limited in scope to the number of monitored endpoints. Assistance can include but is not limited to the following:

- Establish the single point of contact for the Incident Response service
- Initiate analysis of Customer's on-premise and cloud infrastructures, which may contain:
    - host data
    - network data
    - malicious code
    - log data, and
    - cyber threat intelligence
- Preliminary analysis and coordination for digital media handling guidance and support
- Preliminary status reporting and action item tracking
- Preliminary overview of required remediation and next steps

Should more than 40 hours of remote Incident Response assistance be required in any year of the Term of Service, Customer can work with their Dell Technologies account manager to purchase additional time. Any unused time at the end of each year of the Term of Service will be forfeited. Time for a future year within the Term of Service cannot be used before the start of the year for which it was purchased.

Project Management

Dell Technologies Services will assign a Project Manager (PM) as a single point of contact ("SPOC") to manage the delivery of this engagement.

- Single point of contact and accountability for successful delivery of the Services.
- Maintain focus on time, cost, and scope.
- Coordinate and facilitate kickoff, status, deliverable review, and closeout meetings.
- Establish and manage the Services schedule, communications, and status reporting.
- Facilitate change management as needed.

- Confirm the Services delivered are in accordance with the Service Description.
- Obtain deliverable and Services completion acceptance from Customer.
- Manage the Customer relationship.
- Project Management activities are conducted remotely.

Subscription billing

The Service provides for monthly subscription billing, which will be indicated on the Original Order Form with the notation 'Subscription' if Customer has opted-in. Otherwise, standard terms and invoicing will apply. The following terms apply to subscription billing:

- Original Order Form will indicate the contract Term and the number of contracted endpoints. The Term of Service thereafter will auto-renew for consecutive identical terms.
- Customer may increase the number of managed endpoints by submitting an order for additional endpoints. These additional endpoints will be combined with Customer's existing managed endpoints to become the new "Total Number of Endpoints."
- Customer will be invoiced in arrears, monthly, for the Total Number of Endpoints managed at the end of the calendar month.
- At no point may Customer reduce the number of managed endpoints to an amount below the Total Number of Endpoints, nor can the Total Number of Endpoints be decreased for invoicing purposes
- A report of Customer endpoints using the Service will be made available to Customer.
- Customer receives a single invoice across all locations (within the same region.)
- Customer is required to provide Dell Technologies with written notice sixty (60) days in advance of termination of Customer's auto-renewed Term of Service.

Data Volume and Use Limitations

The Service utilizes the Customer's Microsoft Sentinel, Azure, and Microsoft Defender XDR tenant and a Customer-hosted, dedicated Azure subscription and workspace for the Service. Customers purchasing this Service are responsible for understanding and managing their own data volume and use limitations, and Dell Technologies Services waives all such related responsibilities or obligations to the Customer. Customer furthermore acknowledges it is responsible for all data storage and compute costs associated with their Azure subscription and Sentinel workspace.

Data Storage Locations

Customers purchasing this offering are responsible for independently determining their data storage location(s). The M365 region and configurated workspace data locations are set within the Customer's Microsoft Azure environment, at the instruction of and as determined by the Customer.

Microsoft Sentinel stores Customer data within the region defined within their workspace configuration. Microsoft stores Customer data in the same geography as the log analytics workspace associated with the Customer's Microsoft Sentinel environment.

Microsoft Sentinel processes Customer data in one of two locations:

- If the log analytics workspace is located in Europe, customer data is processed in Europe.
- For all other locations, customer data is processed in the United States.

Service Levels

Dell measures its threat response and resolution performance against a number of service levels.

Metric	Definition	Objective
Mean time to react	The average amount of time measured from the time a high or critical alert is generated to the time an investigation is created in the XDR application.	15 minutes
Mean time to respond	The average amount of time measured from the time an investigation is created to the time a Dell analyst provides initial incident analysis in the XDR application or provides a response to Customer.	60 minutes
Mean time to resolve	The average amount of time measured from the time an investigation is created in the XDR application to the time that investigation is resolved.	24-48 hours (requires Customer collaboration)

Assumptions

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

1. All information provided by Customer regarding site technical requirements and architecture is materially correct.
2. Dell Technologies Services will only implement Service-related Security Configuration changes permitted by the Dell Change Management process.
3. Dell Technologies Services is not liable for any policy changes that the customer implements without following the Change Management process.
4. The Services described in this Service Description will be executed remotely.
5. Dell Technologies Services is managing the environment via Microsoft Sentinel dashboards.
6. The product capability is dependent on the Microsoft license and subscription that Customer has purchased to protect Customer workloads; this will impact the Dell Technologies Services team's available remediation options.. For example, to protect Severs, Defender for Server Plan 1 is the recommended minimum baseline. However, servers will benefit from additional protections from Defender for Server Plan 2, which adds additional Microsoft Defender for Cloud capabilities.
7. Dell reserves the right to change the Case Management/ITSM solution as new capabilities are released.
8. Customer endpoint counts will be calculated based on the number of endpoints monitored in Sentinel.
9. Dell Technologies Services will move a customer from SOC onboarding to steady state monitoring once a minimum of 40% of endpoint sensors to have been deployed to the licensed endpoints.
10. In the event this Service will not be completed within the described period of time, Dell Technologies Services reserves the right to assess the root cause. If the root cause is outside of Dell Technologies Services' control, Dell Technologies Services will propose steps to deal with the delay. Those steps may require Customer to purchase additional services or incur additional expenses in order to allow Dell Technologies Services to complete this Service. Should the

Customer have additional requirements outside the scope of this Service Description, assistance with these requirements would be proposed as an additional service for an additional fee.

11. The Microsoft Sentinel ecosystem has high signal-to-noise ratio and therefore low false positives; Dell Technologies Services will investigate informational and low severity alerts based upon high volume of the same type of alert, prioritized after investigating High and Medium alerts.

Exclusions

While the Service is intended to assist Customer to identify and reduce risk, it is impossible to completely eliminate risk. Therefore, Dell Technologies Services makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur in the Customer IT environment.

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

1. Any services, tasks or activities other than those specifically noted in this Service Description.
2. The Service does not include the development of any intellectual property created solely and specifically for the Customer.
3. Troubleshooting or fixing any existing system / server problems unless otherwise described in this Service Description, including but not limited to M365 Defender sensors or Microsoft Sentinel supported agent defects
4. Testing integration between a Dell Technologies product and other third-party products, such as, but not limited to, third-party encryption or security products.
5. Remediation or mitigation of any of the performance issues identified by the analysis of the Customer environment unless otherwise described in this Service Description.
6. Dell Technologies Services responsibility (including financial responsibility) for any Customer and/or third-party personnel, hardware, software, equipment or other assets currently utilized in the Customer's operating environment, unless otherwise set forth in this Service Description.
7. Resolution of compatibility issues or other issues that cannot be resolved by the manufacturer or for configuring hardware, software, equipment, or assets in contradiction to the settings supported by the manufacturer.
8. Monitoring of informational and low severity alerts are not in scope of this Service.
9. Installation of; or configuration of, syslog servers or syslog/CEF collectors
10. Configuration of Microsoft Defender for Cloud Apps applications.
11. Monitoring of Microsoft Defender for Cloud features that are not included in the Microsoft Defender for Servers Plan 1 or Plan 2 License.
12. Monitoring of any servers which have not been onboarded as part of the Service. Dell Technologies will not triage alerts related to any entity other than onboarded servers.
    a. Note: This is only applicable to in scope servers / Defender for Cloud.

Offer-Specific Customer Responsibilities

Customer agrees to cooperate with Dell Technologies Services in its delivery of the Services, and agrees to the following responsibilities:

1. Follow the Change Management process for requests to make changes in the XDR platform, and provide Dell Technologies Services with the Customer contact that will approve Change Management requests.
2. Provide the Dell Technologies Services analyst with access to all required Customer environments for the Term of the Service.
3. Provide a Customer-nominated representative who will be present and available for all planning and review sessions.
4. Provide all authorizations, including third-party authorizations, required to permit Dell Technologies Services to manage the XDR platform on Customer's behalf.

5. Deploy agent/sensor(s) to all of the customers licensed endpoints utilizing appropriate application deployment tools (such as Intune, SCCM, etc).
6. Participate as appropriate in the provision of the Service. Customer understands that without proper participation, including goal setting, the technician cannot work towards meeting Customer needs or perform the Service.
7. Cooperate with and follow the instructions given by Dell Technologies Services analysts.
8. Review and agree to pre-engagement checklists and test plans.
9. Ensure Customer IT environment has a supported endpoint agent that is installed on a host that is licensed for Service.
10. Obtain all support for third-party endpoint agents from the third-party or other authorized sources; Dell Technologies Services does not provide support for third-party endpoint agents.
11. Remove or add an exception for conflicting first- and/or third-party antivirus and EDR agents as necessary for Dell Technologies Services to provide this Service.
12. Ensure availability of and access to sufficient network bandwidth to perform the Service.
13. Ensure all device integrations function and continue to function appropriately. If Customer requires, Dell Technologies Services can help with this for a fee.
14. Provide appropriate access to XDR applications for integration(s).
15. Ensure Customer security controls are compatible with XDR integrations.
16. Manage credentials and permissions for integrations with XDR application.
17. Ensure list of Customer authorized contacts remains current, including permissions and associated information.
18. Provide prompt information and assistance (e.g., files, logs, IT environment context) during threat investigations by Dell Technologies Services.
19. Identify and authenticate all Customer-authorized users of the Service.
20. Control against unauthorized access by users, and maintain the confidentiality of usernames, passwords and account information.
21. Responsibility for all activities by Customer-authorized users, and will notify Dell immediately of any unauthorized use of the Service.
22. Use of two-factor authentication, where available, to access the Service.
23. Accept all updates and upgrades to the Endpoint Agent necessary for the proper function and security of the Service.
24. Provide Dell Technologies with service outage windows as needed.
25. Control data access to prevent cross-client data pollination, and to limit data loss or data leak risks in Customer's environment.
26. Maintain an accurate number of managed endpoints supported by the Service.
27. Setup of Microsoft Sentinel Azure Subscription and provisioning of access needed by Dell analyst. This is a prerequisite of the Service.
28. Provide access to Microsoft 365 Defender via Microsoft Sentinel will be provisioned via Microsoft Entra ID B2B invites sent by Customer to Dell Analysts.
29. The physical and network security of Customer environment.
30. Providing all documentation on DT Services standard templates unless both parties agree otherwise.
31. Provide at least two (2) levels of escalation contacts to respond timely to Dell escalations. Customer is expected to provide escalation contacts available during holidays and business closure.
32. Maintain the health, tuning and configuration of the Microsoft Sentinel dashboards.
33. Submitting technology support tickets to Microsoft for resolution. Dell Technologies Services does not provide support for third-party endpoint agents.
34. Determine how much of Customer's security data to ingest into Microsoft Sentinel.
35. Monitor alerts generated for non-server entities.

36. Removal of any First- / Third-party AV/EDR agent.
37. Provide DT Services with any required consents necessary to perform the Service
38. All data retention and compute costs.
39. Configure the policy settings to meet the Customer's needs.
40. Add integrations and data sources to the managed MDR platform.
41. Provide a dedicated Azure Subscription is needed to provide Case/Incident Management, Investigations, and Quarterly Reports via Microsoft Sentinel.
42. Onboarding Android and iOS devices. Please note that each phone being monitored counts as an endpoint being monitored as part of this Service.

Glossary

Table: 3

Term	Description
Alert	Prioritized occurrences of suspicious or malicious behaviour observed by the MDR application.
Case Management	Centralized platform used for investigating and managing security incidents and alerts.
Change Management	The controlled identification, implementation, and approval of required changes within a customer environment.
Endpoint Agent / Sensor	An application installed on an endpoint that is used to gather and send information about activities and operating system details of the endpoint to the security application for analysis and detection of threats.
Endpoint Detection and Response ("EDR")	A security platform using the first party endpoint agent to monitor end-user devices − desktops, laptops, tablets and phones − for threats that antivirus software cannot detect.
Extended Detection and Response ("XDR")	A detection and response platform that extends beyond just the traditional endpoint (cloud, OT, network, etc.). XDR platform uses integrations or connectors to ingest native, third party, or service oriented data that gets cross-correlated for security monitoring context.
Incident Response	Response actions taken to mitigate an identified security incident.
Integration	Application Programming Interface (API) calls or other software scripts for conducting the agreed-upon Services for the connected technology.
Investigation	A central location that is used to collect evidence, analysis, and recommendations related to a threat that may be targeting an asset in Customer IT environment.

Managed Detection and Response Application (“MDR”)	Security application supported by the Dell MDR offer. For technical details refer to Technical Data Sheet.
Security Incident	A circumstance in which a compromise or suspected compromise has occurred involving Customer.
Security Policy	Policies of the XDR Platform that enforce the prevention and detection settings within the customer environment.
Security Configuration	40 hours per quarter service included in MDR that provides customers with investigation or alert related response actions.
Tenant Enablement & Readiness	Provide guidance on core components needed to enable the Services. Tenant Enablement & Readiness is designed to make sure the Customer’s IT environment meets the minimal required configurations to provide 24/7 monitoring.
Threat	Any activity identified by the MDR application that may cause harm to an asset in Customer IT environment.
Threat Hunting	The cyclic process in which both the software and humans seek previously unidentified threats within an IT environment.
Threat Response	In-platform responses available on the XDR application such as isolate host or block file (containment type action).

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.

Excluded Data. Excluded Data" means: (i) data that is classified, used on the U.S. Munitions list (including software and technical data); or both; (ii) articles, services, and related technical data designated as defense articles and defense services; (iii) ITAR (International Traffic in Arms Regulations) released data; and (iv) personally identifiable information that is subject to heightened security requirements as a result of Customer's internal policies or practices, industry-specific standards or by law. Customer acknowledges that the Service is not designed to process, store, or be used in connection with Excluded Data. Customer is solely responsible for reviewing data that will be provided to or accessed by Dell Technologies Services to ensure that it does not contain Excluded Data.

Service Hours. Subject to local law relating to weekly work hours, unless otherwise listed below, Tenant Enablement & Readiness Services will be performed Monday through Friday during normal Dell Technologies Services business hours, which is from 8:00 AM to 6:00 PM Customer local time:

Country	Normal Dell Technologies Services Business Hours
St. Kitts, St. Lucia, St. Vincent, Trinidad, Virgin Islands, Rest of English speaking Caribbean	Monday thru Friday from 7:00 AM to 4:00 PM
Barbados, Bahamas, Belize, Costa Rica, Denmark, El Salvador, Finland, Grand Cayman, Guatemala, Honduras, Jamaica, Norway, Panama, Puerto Rico, Rep. Dominicana, Suriname, Sweden, Turks and Caicos	Monday thru Friday from 8:00 AM to 5:00 PM
Australia, Bermuda, China, Haiti, Japan, Netherland Antilles, New Zealand, Singapore, Thailand	Monday thru Friday from 9:00 AM to 5:00 PM
Argentina, Brazil, Ecuador, France, India, Indonesia, Italy, Korea, Malaysia, Mexico, Paraguay, Peru, Taiwan, Uruguay	Monday thru Friday from 9:00 AM to 6:00 PM

Bolivia, Chile	Monday thru Friday from 9:00 AM to 7:00 PM
Middle East	Sunday thru Thursday from 8:00 AM to 6:00 PM
Hong Kong	Monday thru Friday from 9:00 AM to 5:30 PM

No Tenant Enablement & Readiness Services 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	Dell.com/CTS	Dell.com/CTS
Canada	Dell.ca/terms (English) Dell.ca/conditions (French-Canadian)	Dell.ca/terms (English) Dell.ca/conditions (French-Canadian)
Latin America & Caribbean Countries	Local on line Commercial Terms of Sale located at Dell.com country-specific website or Dell.com/servicedescriptions/global.*	Service Descriptions and other Dell Legal Entity service documents which you may receive from your seller shall not constitute an agreement between you and Dell Legal Entity but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other Dell Legal Entity service document shall in this context be understood as a reference to you whereas any reference to the Dell Legal Entity shall only be understood as a reference to a Dell Legal Entity as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with the Dell Legal Entity with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.
Asia-Pacific-Japan	Local Dell.com country-specific website or Dell.com/servicedescriptions/global.*	Service Descriptions and other Dell Legal Entity service documents which you may receive from your seller shall not constitute an agreement between you and the Dell Legal Entity but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other Dell Legal Entity service document shall in this context be understood as a reference to you whereas any reference to the Dell Legal Entity shall only be understood as a reference to a Dell Legal Entity as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with the Dell Legal Entity with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.

Asia-Pacific-Hong Kong	https://www.dell.com/learn/hk/zh/hkcorp1/legal_terms-conditions_dellgrmwebpage/commercial-terms-of-sale-hk-en-zh?c=hk&l=zh&s=corp&cs=hkcorp1	Service Descriptions and other Dell Legal Entity service documents which you may receive from your seller shall not constitute an agreement between you and the Dell Legal Entity but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other Dell Legal Entity service document shall in this context be understood as a reference to you whereas any reference to the Dell Legal Entity shall only be understood as a reference to a Dell Legal Entity as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with the Dell Legal Entity with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.
Europe, Middle East, & Africa	Local Dell.com country-specific website or Dell.com/servicedescriptions/global.* In addition, customers located in France, Germany and the UK can select the applicable URL below: France: Dell.fr/ConditionsGeneralesdeVente Germany: Dell.de/Geschaeftsbedingungen UK: Dell.co.uk/terms	Service Descriptions and other Dell Legal Entity service documents which you may receive from your seller shall not constitute an agreement between you and the Dell Legal Entity but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other Dell Legal Entity service document shall in this context be understood as a reference to you whereas any reference to the Dell Legal Entity shall only be understood as a reference to a Dell Legal Entity as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with the Dell Legal Entity with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.

* Customers may access their local Dell.com website by simply accessing 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.

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/servicedescriptions/global.

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 or DellEMC.com website in connection with your purchase or within a Dell Technologies 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.

Data Collection and Use Notice

This Notice ("Notice") explains how Dell Technologies and its group of companies, on behalf of itself or for a third party or for its direct and indirect subsidiaries ("Dell"), collects, uses and shares your data when you use Dell software. We collect and use certain types of data, described below, to personalize your experience with Dell products, to enhance our support and to improve our products, solutions and services ("Dell Solutions").

Information We Already Collect. We may automatically collect behavioral and usage information about how you use, access or interact with the Dell Solutions. This information may not necessarily reveal your identity directly but may include unique identification identifier and other information about the specific device you are using, such as your service tag, the hardware model, operating system version, hardware settings and system crashes, installed applications, their settings and usage, and/or (MAC) address, and other data that may uniquely identify your device or system.

We may also collect information about how your system or device has interacted with the Dell Solutions, such as statistical information, network connection indicators and routing, or in the case of the Dell Service, information related to security events. In some instances, the information collected may directly or indirectly identify an end-user and link an individual to certain online behavior to the extent required for the purposes provided in this Notice.

In order to support these activities, you agree to grant Dell a limited, nonexclusive license to use your data to perform the Service. You also agree to grant Dell a limited, non-exclusive, perpetual, worldwide, irrevocable license to use and otherwise process data related to security events during and after the Term of Service to develop, enhance and/or improve the Service and the Dell Solutions we offer and provide to our customers. Dell is not required to return or delete data related to security events upon termination of the Service for any reason.

[Dell software may consolidate all or part of the aforementioned information in data logs that are transmitted to Dell when an internet connection is established.]

The types of technology used by Dell may change over time as technology evolves. For more information about our use of cookies and other similar tracking technologies please read our Cookies and Similar Technologies on Dell's online Privacy Statement.

Data Transfers. Data described in this Notice may be transferred outside of your country to other locations such in the USA, EU, Japan, including to third party hosting sites. We will take all appropriate technical and organizational measures to safeguard the data that we transfer.

Retention of Your Data. We will retain your personal data as necessary in connection with the purposes described in this Notice, and in accordance with Dell's retention policies and applicable law. The data that is collected by Dell as described in this Notice will be kept in accordance with Dell's retention policies and applicable law.

Personal Information and Privacy. Dell's collection, use and processing of Personal Information you provide is described in Dell's Privacy Statement. If you would like to contact us for any reason regarding our privacy practices, please email us at privacy@dell.com or see our full Privacy Statement online at https://www.dell.com/learn/us/en/uscorp1/policies-privacy-country-specific-privacy-policy

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 Service. 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 own 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 by 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, Service features and functionality, 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.