Service Description

Managed Detection and Response for Infrastructure Systems

Introduction

Dell Technologies Services is pleased to provide Managed Detection and Response service for Infrastructure systems (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.

Managed Detection and Response service provides managed cybersecurity services of the Customer storage appliances with 24/7 monitoring, detection, response, and security incident management by Dell's security operations center (SOC) experts. The MDR Service leverages the CrowdStrike Falcon Platform that gives high visibility fo

r Dell's SOC experts to monitor and protect the Customer environment from attacks and breaches.

The MDR Service is limited in scope to the Platform modules specified below:

- CrowdStrike Falcon Prevent (next-gen anti-virus, "NGAV")
- CrowdStrike Falcon EDR (unlimited data ingest and 60 days raw data retention)
- CrowdStrike Next-Gen SIEM/XDR (4GB per month data ingest and 60 days raw data retention)
- Threat Intelligence
- CrowdStrike Threat Graph (60 days retention)
- CrowdStrike Falcon Data Replicator (FDR)

The Scope of This Service

The Service seeks to provide the Customer with Managed Detection and Response services. The Service is provided remotely. Key components of the Service are described in table 1 below:

Table: 1

Service purchased	Key components of the Service
Managed Detection and Response	• Service provided on CrowdStrike Falcon Platform • Operating hours: 24 hours a day, 7 days a week (24x7) • Onboarding

Internal Use - Confidential

	• Detection • Threat Response • Service-related Security Configuration • Quarterly Reporting • Incident Response

Managed Detection and Response - Service-Only	• Includes above components, leveraging Customer currently licensed CrowdStrike Falcon Platform account.
	• Subscription only.
	• Customers purchasing the MDR service-only offer must procure the modules listed below to receive Services*:
	  ○ CrowdStrike Falcon Prevent (NGAV)
	  ○ CrowdStrike Falcon EDR
	  ○ CrowdStrike Next-Gen SIEM/XDR
	  ○ CrowdStrike Falcon Data Replicator (FDR)
	*Dell recommends that the customer have at least 60 days of retention and 4GB ingestion, as well as CrowdStrike's Threat Intelligence and Forensics modules.
	**Service only not supported for MDR for Data Protection or Unstructured Data Solutions

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.

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

Table: 2

Key Component	Elements
Onboarding	• Service initiation meeting (kick off meeting) • Customer completed pre-engagement checklist • Review Customer IT Environment • Platform enablement • Platform configuration guidance
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
Quarterly Report	• Reporting on investigations • Alert trends analytics

Internal Use - Confidential

	• Security posture guidance
Incident Response	• Remote Incident Response initiation
Project Management	• Manage delivery of this engagement

Detailed Description

Onboarding:

Service initiation meeting
A Dell Technologies Services Project Manager will call for a meeting to review Service expectations and requirements with Customer 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 Platform (see definition in Table 5, below) and how they can be applied to the Customer.
- Provide guidance on vendor supported Platform integrations with 3rd 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 existing IT environment into which the software will be implemented.

Platform application enablement

- Establish Customer designated instance of the Platform applications to initiate Service
- Send Customer the initial application registration for access to the Platform
- Provide Customer with access to the required appliance Agent(s), or log collection software as necessary

Platform configuration guidance
Advise Customer through how to deploy and configure the Platform.
The following activities are included in onboarding the Service:

- Guidance with obtaining deployment packages
- Guidance with security policy configuration
- Guidance for deployment of log capture components*
- Guidance in the remediation of deployment related issues in the Platform

*Log capture components are only used with MDR for Data Protection.

Detection

Internal Use - Confidential

24x7 Access to Security Analysts
Dell Technologies Services security analysts are available on a 24x7 basis to Customer.

Threat Detection and Investigations
Review and investigate threats detected within the Platform. Threats requiring further analysis as determined by Dell Technologies will result in the creation of an Investigation within the Platform. Dell Technologies will contact Customer through the IT service management ("ITSM") 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 Platform and supported Integration. 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 ITSM portal, email, or supported integrations.

Threat Response

During onboarding, Customer will pre-approve select Threat Response action recommendations which may be taken as part of the Service. Dell Technologies Services will perform Threat Response actions if available, and if not send along recommended suggestions leveraging the CrowdStrike Platform.

Service-related Security Configuration

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

- MDR integration (Log Collection or API integration) troubleshooting and best practice guidance.
- Guidance regarding updates to Platform policies (including NGAV policy).
- Guidance configuring and integrating third-party on applications into the 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 Report

Dell Technologies Services will provide quarterly reporting on trends and notable activity observed within Customer's IT environment through the Platform and provide recommendations on how to defend against potential threats. The quarterly report includes a review of investigations, alert trends and analytics, as well as guidance regarding the Customer's security posture.

Internal Use - Confidential

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 appliances. 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-premises and cloud infrastructures, which may contain:
    - host data
    - network data
    - malicious code
    - log data
    - 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 kick-off, 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:

Internal Use - Confidential

- Original Order Form will indicate the contract Term and the number of contracted appliances. The Term of Service thereafter will auto-renew for consecutive identical terms.
- Customer may increase the capacity and or number of appliances by submitting an order for additional capacity or number of appliances to be added. This additional capacity or number of appliances will be combined with Customer's existing managed appliances to become the new "Total Capacity or Number of Appliances."
- Customer will be invoiced in arrears, monthly, for the Total Capacity or Number of Appliances managed at the end of the calendar month.
- At no point may Customer reduce the number of managed appliances to an amount below the Total Capacity or Number of Appliances, nor can the Total Capacity or Number of Appliances be decreased for invoicing purposes.
- A report of Customer endpoints using the Service will be made available to Customer.
- Customers receive 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.

Supported Dell Storage Appliances:

Data Protection:

Dell Power Protect Data Domain:

- Supported Power Protect Data Domain Appliances are based on supported DDOS revision see Technical Data Sheet for details and amendments
- Data Domain Virtual Edition is supported by custom offer

Power Protect Data Manager software

- Power Protect Data Manager software is supported by specific version see technical data sheet for details and amendments
- DM appliances are not supported

Unstructured Data Systems:

Power Scale with Superna + Data Security

- All currently supported Power Scale nodes are applicable see Technical Data sheet for details and amendments
- Superna is Required but only the Security module or some combination of modules that include the security module.

Early Termination (for Latin America & Caribbean Countries only)

In jurisdictions where early termination of services for convenience is permitted under local law, early termination by Customer of the Service will not entitle the Customer to a refund for amounts already paid for the Service, whether paid in monthly installments or in full time of purchase. Furthermore, Customer shall be responsible for all remaining monthly payments owed under the originally agreed Term of Service. The Customer payment obligations described in this section shall be made in consideration for the investments made by Dell Technologies Services to provide the Service.

Internal Use - Confidential

Data Volume and Use Limitations

If the amount of Customer data collected in any given month exceeds the use limit by up to 10%, Dell Technologies Services will notify Customer, and a 30-day billing grace period will be granted so that corrective action may be taken, and Customer can avoid being invoiced a data storage fee. If, for a period of 12 (twelve) months from the Customer's first instance of exceeding the use limit, the amount of data collected exceeds the use limit by up to 10% again, Customer will be charged a data storage fee covering the period of time from the first instance of exceeding the use limit to the subsequent, new instance.

Detection alerts within the CrowdStrike platform have 12 months of data retention

Customers purchasing the Managed Detection and Response - Service-Only offering 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.

Data Storage Locations

The data storage location of the XDR application is in the United States of America (USA) by default for all customers. Customers located in the European Union (EU) will have their Platform application data stored within the EU by default.

Customers are permitted only one data storage location for their Platform application data. Data storage locations will remain the same for the duration of the Term.
Customers purchasing the Managed Detection and Response - Service-Only offering are responsible for independently determining their data storage location(s).

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

Internal Use - Confidential

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:

- All information provided by Customer regarding site technical requirements and architecture is materially correct. Dell Technologies Services will only implement Service-related Security Configuration changes permitted by the Change Management process.
- Dell is not liable for any policy changes that the customer implements without following the Change Management process.
- The Services described in this Service Description will be executed remotely.
- Customer's environment may include equipment that is out of warranty. Customer understands the risks of servicing affected equipment. There will be no escalation, hardware break/fix, or troubleshooting of any kind for equipment as part of the Service.
- Customer ad-hoc service requests (request not related to an ongoing incident) must be submitted through formal communication channels only.
- As part of this Service, Dell Technologies Services maintains administrative control of the Platform. Customers have the right to request administrator access but accepts all liability should a security incident or systems outage occur as a result of the Customer having such administrator access. Dell Technologies Services reserves the right to decrement Service-related Security Configuration hours as needed to assist in recovery of any such incident or systems outage.

Exclusions

While the Service is intended to assist Customer to identify and reduce risk, it is impossible to completely eliminate risk, and 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:

- 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.
- Troubleshooting or fixing any existing system / server / Storage Appliance problems unless otherwise described in this Service Description.
- Testing integration between a Dell Technologies product and other third-party products, such as, but not limited to, third-party encryption or security products.
- Remediation or mitigation of any of the performance issues identified by the analysis of the Customer environment unless otherwise described in this Service Description.
- 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.
- Installation of the Platform software on Customer's on-site environment.
- 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.

Internal Use - Confidential

- Purchase of software or software as a service license which are not explicitly included as part of this Service.
- Monitoring of informational and low severity alerts.
- Monitoring of alerts from additional CrowdStrike modules not listed as in-scope for the Service.

Offer-Specific Customer Responsibilities

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

- Follow the Change Management process for requests to make changes in the Platform and provide Dell Technologies Services with Customer contact that will approve Change Management requests.
- Provide the Dell Technologies Services analyst with access to all required Customer environments for the Term of the Service.
- Provide a customer-nominated representative who will be present and available for all planning and review sessions.
- Provide all authorizations, including third-party authorizations, required to permit Dell Technologies Services to manage the Platform on Customer's behalf.
- Deploy supported connection methods to the contracted appliances.
- Participate as appropriate in the provision of the Service. Customers understand that without proper participation, including goal setting, the technician cannot work towards meeting Customer needs or perform the Service.
- Cooperate with and follow the instructions given by Dell Technologies Services analysts.
- Review and agree to pre-engagement check lists and test plans.
- Ensure Customer IT environment has supported connection methods installed on appliances licensed for Service.
- 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.
- 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.
- Ensure availability of, and access to, sufficient network bandwidth to perform the Service.
- Ensure all device integrations function and continue to function appropriately. If Customer requires, Dell Technologies Services can help with this for a fee.
- Provide appropriate access to applications for integration(s).
- Ensure Customer security controls are compatible with Platform integrations.
- Manage credentials and permissions for integrations with the Platform
- Ensure list of Customer authorized contacts remains current, including permissions and associated information.
- Provide prompt information and assistance (e.g., files, logs, IT environment context) during threat investigations by Dell Technologies Services.
- Identify and authenticate all Customer-authorized users of the Service.
- Control against unauthorized access by users, and maintain the confidentiality of usernames, passwords and account information.
- Customer is responsible for all activities by Customer-authorized users and will notify Dell immediately of any unauthorized use of the Service.
- Use of two-factor authentication, where available, to access the Service.
- Accept all updates and upgrades to the connection methods as necessary for the proper function and security of the Service.
- Make appropriate service outage windows available for Dell Technologies Services, as needed.

Internal Use - Confidential

- Control data access to prevent cross-client data pollination, and to limit data loss or data leak risks in Customer's environment.

Glossary

Table: 5

Term	Description
Alert	Prioritized occurrences of suspicious or malicious behaviour observed by the MDR application.
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.
Log Capture	A syslog server will be set up to collect logging data from the Dell storage appliances for transmission to the CrowdStrike Falcon platform and NG SIEM components.
Managed Detection and Response Application ("MDR")	Security application/Platform supported by the Dell MDR offer.
Platform	The software and the complete set of modules required, including the integration and automation required to deliver the Service.
Storage	A server node that contains or attaches too collections of hard drives that act as a centralized pool of space for data. Also a

Internal Use - Confidential

	collection of servers with disks that act as a single entity or locations for data
Security Incident	A circumstance in which a compromise or suspected compromise has occurred involving Customer.
Security Policy	Policies of the-Platform that enforce the prevention and detection settings within the customer environment.
Service-related Security Configuration	40 hours per quarter service included in MDR that provides customers with investigation or alert related response actions.
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 Platform 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.

Internal Use - Confidential

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.

Internal Use - Confidential

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.

Internal Use - Confidential

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.

Internal Use - Confidential

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 Managed Detection and Response 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

Internal Use - Confidential

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.

Internal Use - Confidential

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.

© 2026 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.

Internal Use - Confidential