

Addendum to Master Services Agreement

- i. This service addendum is made pursuant to the Master Services Agreement (The “Agreement”) between (1) the customer (who is identified in the accompanying electronic rider, the terms of which are explicitly incorporated herein) and the customer’s affiliates (collectively the “Customer”) and (2) Dynamic Quest, LLC (“Dynamic Quest”).
- ii. Term of Service: This Addendum will remain in effect until the termination date of the Agreement.

Description of the Service

Mobile Device Management (MDM) is a security service that ensures all equipment accessing the Customer network meets the Customer security criteria. Equipment that does not meet the Customer security criteria are prevented from accessing the Customer network through the MDM technology.

- 1) Mobile phones, tablets and workstations can be enrolled into the MDM service.
 - a) Servers and conference room equipment cannot be enrolled into the MDM service.
- 2) Company owned equipment and user owned equipment (called Bring Your Own Device or BYOD) can be enrolled into the MDM service.
- 3) The MDM technology will download software to the user equipment to provide the MDM service.
- 4) Equipment must be enrolled via the MDM service technology to qualify to be an MDM service.
- 5) Equipment and Operating System versions: Please see exclusions in the Limitations section.
- 6) Privacy:
 - a) No personal data is monitored, captured or viewed. This includes, but is not limited to photos, telephone calls, internet usage, texts, files or app use.
 - b) Please request our Privacy Document from Sales for more details regarding the data used by the MDM service.
- 7) MDM only protects and manages company data. Personal data is not protected or managed.
- 8) Each user may enroll up to five (5) pieces of equipment (Company owned and BYOD combined).
- 9) Features available from MDM:
 - a) Confirm each MDM enrolled equipment meets the security policies selected by the Customer.
 - i) Equipment that does not meet the Customer’s security policies will be denied access to the Customer network until the equipment meets the Customer’s security policies.
 - b) For BYOD equipment, the enhancements provided by MDM pertain only to access to the Customer network and the access to Customer data.

- i) A user's personal settings and applications will still be available on the BYOD equipment.
- c) Enforce password policies or the use of PINs, facial recognition or multi-factor authentication for access to applications or to the Customer network.
- d) Applications
 - i) Automatically push applications, application configurations and application updates as required by the Customer.
 - (1) Applications must be available in the equipment App Store.
 - ii) Protect the data used in the applications by preventing data from being backed up from a protected application.
 - iii) Restrict the copy and paste function to prevent company data being copied from Company applications to non-Company applications.
 - iv) Establish security policies to secure Company data on equipment not owned by the company (BYOD).
 - v) Automatically remove applications no longer utilized by the Company from equipment.
- e) For internet use, MDM can:
 - i) Block all downloads.
 - ii) Limit all cookies to the current browsing session.
 - iii) Delete browsing history.
- f) Restrict use of the hardware camera and/or blue tooth capability on equipment.
- g) Wi-Fi: Configure equipment to automatically connect to company Wi-Fi when the equipment is in range, without the User entering a password.
- h) Lost equipment (actions require the equipment to be connected to the internet):
 - i) Suspend equipment access to the Customer network when the equipment has not connected to the Customer network in XX (to be determined by the Customer) days.
 - ii) Enable "find my device" on Customer equipment, if supported by the equipment and the feature is enabled on the equipment.
- i) Deleting data from equipment:
 - i) This function can only be performed when the equipment is connected to the internet.
 - ii) This function requires authorization from:
 - (1) Customer administrator for Customer owned equipment; or
 - (2) BYOD owner for BYOD equipment.
 - (3) Authorization must be submitted via a trouble ticket.

This service description explains the service to be provided by Dynamic Quest. This service description may be adjusted at any time by Dynamic Quest for accuracy. Please contact your sales representative or go to our on-line service description site for the latest service description.

https://info.dynamicquest.com/service_description

Service Set-up

- 1)) The Customer will:
 - a) For User Groups:
 - i) Select the user groups they want to use from the standard groups provided by Dynamic Quest; and/or,
 - ii) Provide requirements for custom user groups if the Customer wants to pay Dynamic Quest to set-up a custom user group; and,
 - (1) Note: Custom user groups are built on specifications provided by the Customer. The selected security features are the sole decision and responsibility of the Customer.
 - iii) No extra charge for using the standard user groups provided by Dynamic Quest. There is an extra charge for a custom user group.
 - b) Assign MDM users to the appropriate user groups. The Customer MDM administrator is to provide this information to Dynamic Quest; and,
 - c) Select the features to be supported by the MDM Service; and,
 - d) Select applications to be used by users for company business; and
 - e) Registration of equipment on MDM:
 - i) Users will self-register their equipment using an app downloaded to the equipment.
 - ii) The user will open the app and enter their work email and email password.
 - iii) Answer a couple more simple questions.
 - iv) The entire process should take four (4) to five (5) minutes.
- 2) Dynamic Quest will:
 - a) Set-up the service with the features requested by the Customer; and,
 - b) Assign the users to the appropriate user group, as directed by the Customer; and,
 - c) Provide instructions to users to self-register.
- 3) The Service set-up does not include:
 - a) Site Surveys; and,
 - b) Migration efforts from another service to this service; and,
 - c) Removing, organizing or arranging files on an endpoint; and,
 - d) Removal or disposing of equipment not owned by Dynamic Quest.

Pricing

Services will be invoiced one (1) month in advance of services provided.

The following billing elements are used to invoice for this service:

- MDM Standard Set-Up – A non-recurring charge for each user being added to the MDM service.
 - The Customer can purchase standard for some users and purchase premium for other users. The total users for standard and the total users for premium, when added together, should equal the total users being added to the MDM service.
- MDM Premium Set-Up - A non-recurring charge for each device being added to the MDM service.
 - The Customer can purchase standard for some users and purchase premium for other users. The total users for standard and the total users for premium, when added together, should equal the total users being added to the MDM service.
- MDM Custom User Group – A non-recurring charge for each custom user group.
- Mobile Device Management (MDM) - Device Management Fee - A monthly recurring charge for each device enrolled in the service.
- Apple Business Manager License for MDM – A monthly recurring charge for Apple licensing for MDM management.
- Android Enterprise License for MDM – A monthly recurring charge for Android licensing for MDM management.
- Google Play Enterprise License for MDM – A monthly recurring charge for Google licensing for MDM management.

Service Limitations

In addition to other limitations and conditions set forth in this Addendum, the following service and support limitations are expressed:

- 1) Except as otherwise stated in this Addendum, requests for configuration, troubleshooting, repair, replacement or warranty services for Customer or user equipment are not included.
- 2) Operating system upgrades are not provided by Dynamic Quest. Operating system upgrades will be delivered by the equipment manufacturer.
 - a) Any issues with the operating system software or caused by the operating system software must be directed to the equipment manufacturer.
- 3) MDM is not an equipment management or monitoring service.
- 4) Equipment / Operating System Exclusion:
 - a) Equipment enrolled in the MDM service must be operating a supported version of the equipment Operating System and the equipment make and model must be on the Dynamic Quest equipment supported list.
 - b) The list of supported operating system versions and equipment make / models is updated as the MDM technology changes.

- c) The list of supported operating system versions and equipment make / model is a separate document published by Dynamic Quest. Please request the document from the Dynamic Quest Sales representative.
- 5) Dynamic Quest expects the use of a fully implemented Microsoft local Active Directory or Azure AD structure, which facilitates and streamlines management, oversight, security, and project implementations. If a reactive support solution requires substantial time to implement due to the absence of a fully implemented Microsoft local or Azure Active Directory structure, Dynamic Quest, at its sole discretion, may bill the extra time as hourly out of scope in accordance with Addendum E (*use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description*).
- 6) Responsibility for workstation, server and network equipment software version upgrades are described in Addendum B (*use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description*).
- 7) Any audit support provided by Dynamic Quest will be in accordance with Addendum F (*use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description*).
- 8) Customer Hardware and Systems must be current in hardware and software standards to support the customer's existing operating environment. This requires : Warrantable, serviceable and able to support and perform Customer's current business operating environment.
- 9) Customer understands that no monitoring service, software product, or training program can fully protect them from digital theft. DYNAMIC QUEST HAS NO OTHER EXPRESS OR IMPLIED GUARANTEES, WARRANTIES, OR CONDITIONS beyond those provided by the Agreement.

Customer Responsibilities

- 1) Customer provides all equipment or the user provides the equipment to be used with the MDM service.
 - a) No equipment is provided by Dynamic Quest as part of the MDM service.
- 2) Customer or equipment user for a BYOD must provide their own data plan, as required by the equipment for operational purposes.
- 3) Customer provides all Microsoft licenses required to operate the MDM service, as specified by Dynamic Quest.
 - a) Licenses can be purchased from Dynamic Quest.
- 4) Customer must designate at least one (1) Customer employee as the MDM Administrator.
- 5) If the Customer selects applications that require subscription or licensing, the Customer is responsible for obtaining the subscription or licensing and providing the necessary information to Dynamic Quest, if required.

- 6) Customer will assist Dynamic Quest in equipment enrollment by providing documentation and instructions provided by Dynamic Quest to the user community.
- 7) Customer must enforce all eligible equipment to access the Customer network utilizing the MDM service.
 - a) Equipment accessing the Customer network but not enrolled in the MDM Service represent an uncontrolled security threat to the Customer's network.
 - b) Dynamic Quest is not responsible for any consequences that arise from equipment entering the Customer network but not enrolled in the MDM Service.
- 8) Customer grants permission for Dynamic Quest to have secure remote access into Customer's network for management, reporting, alerting, and support functionality.
- 9) Customer will promptly notify Dynamic Quest of any events/incidents that could impact the services defined within this Addendum and/or any supplemental service needs, and for Dynamic Quest to respond in a timely manner via phone, email, and/or remote access.
- 10) Customer agrees that it will inform Dynamic Quest of any modification, installation, or service performed on the Network by individuals not employed by Dynamic Quest to assist Dynamic Quest in providing an efficient and effective Network support response.
- 11) Customer grants permission for Dynamic Quest to become the CSP (Customer Service Provider) for Microsoft Office 365 licenses, Microsoft 365 licenses, and any instances of Azure Hosting. Dynamic Quest will provide for the management and troubleshooting of any issues as well as Tier One helpdesk. Being the Microsoft assigned CSP allows Dynamic Quest to provide the quickest and most proactive levels of support for our Customers.
- 12) All Dynamic Quest owned equipment:
 - a) The Customer is responsible for providing space for the equipment that meets the following criteria:
 - b) Kept inside a climate-controlled, dry area that is protected from the weather. The climate-controlled area must maintain a temperature between 50 degrees Fahrenheit and 80 degrees Fahrenheit; and,
 - c) The climate-controlled area must be kept at a humidity between 50% - 80% and provides air flow; and,
 - d) The area cannot be under construction or have excessive dust.
 - e) Customer is responsible to provide power for the equipment. The power must be in compliance with local electrical regulations. The Customer is responsible for knowing the electrical regulations pertaining to their location; and,
 - f) Customer will provide power conditioning and battery backup for the Appliances; and,
 - g) Customer will provide two (2) gigabit network drops and two (2) internal static IP addresses for each piece of Dynamic Quest provided equipment; and,
 - h) Equipment must be kept in a location that is secure so that only authorized personnel can access the equipment.
 - i) Equipment must be installed in a telecom rack and the rack must be properly installed.
- 13) The Customer is responsible for 3rd party fees for products, software, services, and subscriptions not expressly provided by Dynamic Quest.
- 14) The Customer is responsible for providing adequate and reliable Internet connectivity including appropriate bandwidth.

- a) All network connections from the Internet Provider (ISP) to the endpoint are minimum 1GB handoffs.
- b) The Customer is responsible for the wiring within the building.
 - i) The wiring type will impact the internet speed for any equipment connected to the wiring.
 - ii) If the Customer selects high speed internet, it is recommended the Customer confirm the internet speed supported by the wiring type.
 - iii) Installing new wiring may be required in order to obtain higher internet speed.
- 15) Cost of consumables, replacement parts, hardware, software, network upgrades, and associated services owned by the Customer.
- 16) Manufacturer warranty parts and labor/services of equipment owned by the Customer.
- 17) Legal use rights to monitor digital credentials.
- 18) For failed server restoration: Customer must have a vendor supported network-based backup solution that produces Full Bare-Metal Recovery Backups (“Proper Backups”).
 - a) In the absence of Proper Backups, Dynamic Quest, will attempt to restore on a best effort basis and at its sole discretion, may bill the recovery time for failed servers as hourly out of scope in accordance with Addendum E *(use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description)*.
- 19) Customer infrastructure equipment (including switches, Wi-Fi, firewalls, and other similar equipment) must be considered business class equipment and not residential-use equipment AND be a Dynamic Quest support brand and model in Addendum A *(use this link to go to the Service Description site with the Addendums: https://info.dynamicquest.com/service_description)*.