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 Addendum

Security Remediation is the act of removing malware or addressing a cybersecurity issue on the Customer network caused by a bad actor.

There are 2 types of Security Remediation:

- Proactive Remediation: The act of remediating something found on the network but which has not yet caused damage or taking steps to improve the security on a network.
    - Proactive Remediation is included in Security Services only if the service description for the security service expressly states Proactive Remediation is included.
- Reactive Remediation: The act of removing malware or addressing a cybersecurity issue caused by a bad actor after a security event has taken place.

Dynamic Quest recommends the Customer develop an Incident Response Plan, a Disaster Recovery Plan and a Security Plan. Dynamic Quest can help the Customer to develop some or all of these plans under a separately funded project.

Qualifications for Complimentary Reactive Remediation

1) Customer must have purchased Managed or Co-Managed Services; and,
2) 100% of all people with access to Microsoft 365 Services are utilizing Multi-Factor Authentication ("MFA"); and,
3) Minimum Microsoft 365 subscription that includes Conditional Access for all users; and,
4) Active Directory Password Policies: The Customer must enforce that all passwords used for network access must have at least fourteen (14) characters, including at least one (1) upper-case, and lower-case, and number; and,
    a. Password history set to twenty-four (24) or more; and,
    b. Maximum Password age must be set to 365 or fewer days (but not zero); and,
    c. Minimum Password age set to one (1) or more days; and,
    d. Account lock-outs duration is fifteen (15) or more minutes; and,
    e. After five (5) failed attempts, the account will be locked out.

5) The Customer must purchase the following Dynamic Quest Security Services and all Services must be active and in use to Dynamic Quest recommended set-up:
    a. Manage, Detection and Response (MDR); and,
    b. End Detection and Response (EDR); and,
    c. Anti-Spam service for email; and,
    d. DNS Filtering; and,
    e. Business Continuity and Disaster Recover (BCDR) service; and,
    f. Managed Firewall; and,
    g. Vulnerability Testing including PEN Testing.
6) The Customer must be in good standing with Dynamic Quest and not have its services suspended by Dynamic Quest or have outstanding payments owed to Dynamic Quest.

Reactive Remediation Limits

Complimentary Reactive Remediation:

If the Customer meets the qualifications for a Complimentary Reactive Remediation, then:

- Complimentary Reactive Remediation is available starting sixty (60) days after all the qualifications are in place and active. The sixty (60) day period when Complimentary Reactive Remediation is not available is called the "Waiting Period".
    - If Reactive Remediation is required during the Waiting Period, the Reactive Remediation work will be executed according to the "Reactive Remediation Invoiced to the Customer" section below.
- After sixty (60) days, one $5,000 credit towards the Reactive Remediation effort per Customer, in a twelve (12) month period, is included in the Manage or Co-Manage service.
    - The Customer must execute a Statement Of Work (SOW) according to the "Reactive Remediation Invoiced to the Customer" section below.
    - The $5,000 credit will be applied to the Reactive Remediation SOW.
- Complimentary Reactive Remediation is not included in the Monitoring service.

Reactive Remediation Invoiced to the Customer:

If the Customer elects to engage Dynamic Quest in a Reactive Remediation effort, then:

- Customer will sign a Statement of Work (SOW) outlining the work to be completed during the Reactive Remediation.
- Customer will purchase a block of hours to fund the Reactive Remediation work.
- The hourly rate for work will be in accordance with Addendum E.
- The payment for the block of hours will be fifty percent (50%) due immediately and fifty percent (50%) due thirty (30) days from the effective date of the SOW.

Dynamic Quest will not be involved in soliciting nor will Dynamic Quest extend terms due to Customer insurance payments being delayed or withheld.

Isolation and Containment Activities

When a security event is identified, Dynamic Quest will immediately start servers, firewall and network isolation, remote access shutdown, all remote sites disconnected from the network and workstation isolation (Isolation and Containment). Dynamic Quest will endeavor to notify the Customer of the event but the most pressing concern is the immediate Isolation and Containment activities.

Isolation and Containment activities are defined by Dynamic Quest and the scope of the activities are defined by Dynamic Quest. The Isolation and Containment activities are not invoiced to the Customer. Isolation and Containment activities are a small part of a Reactive Remediation process.

Activities Performed During Reactive Remediation

Reactive Remediation work requires a Customer signed SOW. Dynamic Quest may provide Reactive Remediation work in good faith prior to the SOW being signed. Good faith work will be part of the SOW when signed. Dynamic Quest is not obligated to perform Reactive Remediation without a signed SOW.

Reactive Remediation efforts include:

1) Initial Isolation and Containment Effort
    a. Server isolation of all Customer servers; and,
    b. Firewall (if provided by Dynamic Quest) and Network Isolation; and,
    c. Remote Access shutdown; and,
    d. All remote sites disconnected from the network; and,
    e. Workstation isolation.
2) Investigation
    a. Ransomware Analysis performed by Dynamic Quest and the Forensic Team provided by the Customer, the Customer's insurance or the authorities.
        i. The Forensic Team is paid for by the Customer.
            1. Dynamic Quest does not provide a Forensic team as part of its remediation service.
        ii. Activities include:
            1. Identify the ransomware; and,
            2. Identify and locate all affected assets on the Customer network.
    b. Server activities include:

i. Check the business continuity backups; and,
ii. Upload server logs; and,
iii. Upload server images.
iv. If, due to the severity of the cyber-attack, Dynamic Quest determines the server must be replaced with new equipment, Dynamic Quest will stop work on the impacted server. The Customer will be responsible for the cost of the replacement of the server hardware, the software and the set-up of the new server.

c. Workstation activities include:
   i. If, due to the severity of the cyber-attack, Dynamic Quest determines any workstation must be replaced with new equipment, Dynamic Quest will stop work on the impacted workstation. The Customer will be responsible for the cost of the replacement of the workstation hardware, the software and the set-up of the new workstation.
d. Review the firewall logs.
e. Microsoft O365 activities include:
   i. Gain access to O365; and,
   ii. Investigate O365 to determine the damage of the cyber-attack.
   iii. New licenses or replacement licenses are to be paid for by the Customer.

3) Remediation
   a. Servers activities include:
      i. Decryption; and,
      ii. Investigate space for scrubbed data; and,
      iii. Rebuild / Restore VMware hosts; and,
      iv. Forensic scans; and,
      v. GPO Review; and,
      vi. Cleanse the data.
   b. Workstation activities include:
      i. Decrypt workstations; and,
      ii. Wipe workstations; and,
   c. Network activities include:
      i. Rebuild the Firewall; and,
      ii. Release isolation, bringing remote sites back onto the network.
   d. Microsoft O365 activities include:
      i. Sign out users or block user access to O365; and,
      ii. Enforce MFA on all account(s); and,
      iii. Reset passwords on all accounts.

4) Recovery: To minimize Customer downtime, Dynamic Quest will decide the best process for recovery activities. The Customer is required to follow the processes provided by Dynamic Quest.

a. Bring servers on-line activities include:
    i. Set up a new server environment; and,
    ii. Build new servers and migrate data; and,
    iii. Server hardening.
    iv. All hardware and software costs plus new server set-up costs are the responsibility of the Customer.
b. Activities for bringing workstations on-line include:
    i. Wipe and reload affected workstations; and,
    ii. Install Dynamic Quest tools; and,
    iii. Application Recovery.
    iv. All hardware and software costs plus new workstation set-up costs are the responsibility of the Customer.
c. Network activities include:
    i. Create a temporary, isolated network for recovery efforts; and
    ii. Harden the firewall; and,
    iii. Review network segmentation and correct any important deficiencies, as determined by Dynamic Quest.
d. Microsoft O365 activities include:
    i. Set-up Conditional Access; and,
    ii. Enforce Multi-Factor Authentication.

5) Forensic Review
    a. Dynamic Quest will work with security firm consultants, hired and paid for by the Customer, throughout the duration of the security event.
    b. Any travel, in person meetings, regulatory meetings, audits or reporting are outside the scope of Reactive Remediation. These activities will be paid for by the Customer, in accordance with Addendum E.
6) Post Incident Review
    a. Review the event and understand the vector of the attack to ensure vulnerable areas are addressed.
    b. Cyber-attacks may be so sophisticated that identifying the vector of the attack or the vulnerable areas is not possible.
    c. These efforts will be a best-effort by Dynamic Quest.

Reactive Remediation Limits

Remediation activities are performed remotely. On-site staff or efforts are not supported unless the Customer agrees to pay for the on-site efforts, in accordance with Addendum E.

Remediation activities are limited to the Dynamic Quest Customer on the Dynamic Quest order form. Other impacted networks that are not part of the Dynamic Quest Customer network are

outside the scope of Dynamic Quests Remediation efforts. Subsidiaries or divisions of the Dynamic Quest Customer whose network is not managed by Dynamic Quest are not included in the Remediation.

During the Remediation effort, the Customer network will cease to operate for a period of time. It is not possible to estimate how many hours, days or weeks the Customer network will not operate. All efforts will be made to make the Customer network operational but only after Dynamic Quest determines it is safe to do so.

Dynamic Quest is not responsible for peripheral equipment, industrial equipment or other equipment not under Dynamic Quest management. Dynamic Quest is not responsible for equipment that is monitored but not managed by Dynamic Quest.

Dynamic Quest is not responsible for notifying or engaging the Customer's cyber-security insurance. The Customer must notify their insurance about the cyber-security event. Any meetings regarding the cyber security event involving the insurance company and Dynamic Quest must be arranged by the Customer and the Customer must attend all meetings.

An Incident Response Plan, Disaster Recovery Plan and Security Plan are not included in the Reactive or Proactive Remediation. These plans can be developed as part of a separately funded project in accordance with Addendum E.

Providing and paying for a Forensic team as part of the Remediation service is the responsibility of the Customer.

All hardware and software costs plus new server set-up costs are the responsibility of the Customer.

Any travel, in person meetings, regulatory meetings, audits or reporting are the responsibility of the Customer.

This Addendum explains the service to be provided by Dynamic Quest. This Addendum 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