# Services Guide

**This Services Guide contains provisions that define, clarify, and govern the services described in the quote (the "Quote") provided to you (the "Customer"). If Customer does not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.**

## Managed Services & Plans

The following Services, if included and accepted by you in the Quote, will be provided to you.

| PLAN LEVELS | GENERAL DESCRIPTION |
|---|---|
| **Basic Care** | **Backups:** Includes Backup Policy #1 with data retention of 30 days and a single daily snapshot. With this backup policy, Customer will have restore options for a single point in time for any of the preceding 30 days. The file version available will only be what was backed up during the single snapshot at the end of that day (if the file changed since the previous snapshot). Files will NOT be available for restore further back than 30 days.<br><br>**Security:** Managed Endpoint Detection/Response (EDR) - Monitors endpoint devices to detect and assist in responding to malicious activity. Intrusion Detection system (IDS) - Monitors network traffic for known or suspected malicious or unauthorized activity and generates alerts for EMD to support network security. Gateway antivirus protection - Provides real-time, firewall-level inspection of network traffic to detect and block viruses, malware, ransomware, and other malicious code before it enters or leaves the network. Botnet filtering - Blocks network traffic to and from known or suspected botnet command-and-control endpoints, reducing the risk of malware activity and unauthorized system control. GeoIP filtering - Allows network traffic to be permitted or blocked based on the geographic source of IP addresses, configured as needed for Customer's needs.[1]<br><br>**Labor:** Provides a limited scope of services designed to address essential support needs. The plan includes coverage for specific, predefined services only and includes up to **five (5) hours per month** of labor exclusively for:<br>• Remediation of security issues identified by EMD's security monitoring platforms<br>• File restoration services, when required<br>• Microsoft 365 tenant audits (applicable only to customers who subscribe to EMD's Microsoft 365 Procurement & Tenant Configuration service)<br><br>Labor coverage under the Basic Care service offering applies solely to incidents that are detected and formally alerted by EMD's security monitoring platforms. Customer-initiated service requests, including those characterized by Customer as "security-related," are expressly excluded unless such incident was first identified through EMD's security monitoring systems. Basic Care does not include labor for general technical support, end-user assistance, network or infrastructure troubleshooting, connectivity issues, or other non-security IT services. Any services exceeding the included monthly hours— including covered cybersecurity incidents identified by EMD's security monitoring platforms— shall be billed at the discounted Basic Care hourly labor rate then in effect. EMD may, at Customer's request and subject to availability, perform additional services outside the scope of Basic Care. All such non-covered services shall be billed at the Basic Care's discounted rates. |

| | |
|---|---|
| **Net Care** | **Backups**: Includes Backup Policy #2 with data retention of 60 days and snapshots every 4 hours, allowing for more restore point options. With this backup policy, Customer will have restore options for multiple restore points from the previous 30 days, plus a single restore point as far back as 60 days. The file version available will depend on which restore point is selected, and the state of the file during that snapshot, allowing for multiple versions of the file to be restored.<br><br>**Security**: Includes all security features in Basic Care plus: Basic DNS filtering – blocks access to domains that could be a threat to your network, and is appropriate for users within an office (not necessarily remote users). External port scanning (requires a public IP address) – tests your network for vulnerable open ports and alerts us so we can secure them. 30 day firewall log retention – longer retention for more detail of activity when needed for problem remediation. [1]<br><br>**Labor**: Includes labor covered under Basic Care, plus advanced troubleshooting and remediation of connectivity issues within the Customer's LAN/WLAN environment. This includes endpoint-to-network connectivity for workstations, printers, and scanners; internet/WAN access issues; Wi-Fi connectivity; VPN and other remote access services for users and third-party vendors; and general network connection failures impacting internal resources. Also includes Microsoft 365 tenant audits when MS365 Procurement & Tenant Configuration is selected. |
| **Total Care** | **Backups**: Includes Backup Policy #3 with data retention of 60 days and hourly snapshots, plus a 1-year snapshot, allowing for even more restore point options. With this backup policy, Customer will have hourly restore options for the previous 30 days, daily restore points for up to 60 days and a single snapshot up to 1 year old.<br><br>**Security**: Includes all security features in Net Care plus: Managed IT hardware and software asset inventory – helps with many standards requirements (ISO, SOC 2, HIPAA, etc.), helps with license requirements, change management and cost control. 90-day firewall log retention for more detail when needed. [1]<br><br>**Labor**: Labor is covered for standard day-to-day IT support needs, including (but not limited to) remote and onsite end-user support; user onboarding and offboarding; new workstation installation and configuration; Microsoft 365 user administration; operating system support (including patch-related issues); vendor liaison services; hardware troubleshooting and resolution (parts not included); mobile device email support; and other related IT support services.<br><br>**Labor is not covered for projects.** A project is defined as any new addition to your network environment—whether hardware or software—or any significant change to the structure, design, or configuration of your existing network. Projects typically involve planning, implementation, configuration, deployment, or migration work that goes beyond routine maintenance or standard support. All projects shall be quoted and approved prior to commencement of work. Labor shall be billed at the applicable Total Care discounted rate.<br><br>Examples of projects include, but are not limited to:<br>• Installing or deploying a new server (on-premises or virtual)<br>• Implementing a new network infrastructure component such as firewalls, switches, or wireless systems<br>• Adding or rolling out a new software application across the organization<br>• Migrating systems, data, or services to the cloud<br>• Performing major upgrades that substantially change system architecture<br>• Office relocations or network rebuilds<br>• Large-scale hardware refreshes<br>• Security redesigns or compliance-driven infrastructure changes<br><br>[1]*Some security features/services require Customer to have a business class router with an active subscription and certain levels of Microsoft 365 licenses. Lack of these requirements will limit our ability to provide some services and may void some features.* |

| STANDARD SERVICES & PLAN SPECIFICATIONS | GENERAL DESCRIPTION |
|---|---|
| **OS Patch Management** | EMD will configure and monitor automated installation of high-priority and critical operating system security patches. EMD will use commercially reasonable efforts to defer or exclude non-essential patches that may reasonably be expected to cause system instability or performance degradation. Operating system patches are developed, issued, and tested by third-party vendors and are not created, modified, or controlled by EMD. Accordingly, EMD shall not be liable for any system outages, performance issues, data loss, incompatibility, or other adverse effects resulting from the installation or operation of such patches. Labor required to diagnose and remediate operating system issues resulting from patch installation is not included, unless explicitly stated in your agreement level description. |
| **EDR + Antivirus** | EMD will deploy and configure a premium business-class Endpoint Detection and Response (EDR) solution integrated with antivirus protection (either the built-in antivirus or EMD-provided antivirus licenses, as required). This solution includes 24/7 advanced monitoring to ensure continuous protection of covered workstations and servers. In the event a threat cannot be automatically removed, EMD will perform manual remediation to eliminate the threat. EMD shall not be held liable for infections resulting from negligent user actions, including but not limited to downloading malicious files or opening email attachments from unknown or untrusted sources.<br>To further reduce the risk of viruses, ransomware, and other cyber threats, and for the most secure email platform, EMD strongly recommends implementing our **Microsoft 365 Procurement & Tenant Configuration** service, along with enrolling users in the **EMD Phishbait** security awareness program. Please note that labor coverage for manual remediation may not be included, may be limited, or may vary depending on your service agreement level. Refer to your agreement plan for specific coverage details. |
| **Monitoring Services** | Using our monitoring software, EMD will continuously scan and monitor your servers, workstations, and other network devices for errors, capacity issues, and overall device health. We receive real-time alerts that allow us to take proactive, preventative action—often avoiding downtime altogether. Drive capacity monitoring is designed to track normal long-term storage growth and alert us before space becomes critically low. However, if a drive fills rapidly due to an unexpected event, the monitoring system may not generate an alert in time before the drive reaches full capacity, which could result in downtime. |
| **Automated Preventative Maintenance** | EMD's monitoring software automatically repairs many system services and processes, helping prevent costly downtime on servers and workstations. If an issue identified by an alert cannot be resolved automatically, EMD will address it manually or provide the Customer with a recommended course of action. |
| **Disk Maintenance** | EMD's monitoring software performs regular automated disk scans and maintenance to help ensure servers and workstations operate efficiently. If an issue is detected that indicates a potential or imminent hardware failure, we will provide a quote for device replacement or recommend an appropriate resolution.<br>Manual file cleanup—excluding system and temporary files—will be billed by the hour unless explicitly covered under the applicable service agreement level. |

| | |
|---|---|
| **Local/Cloud Backups & Retention Policies** | Local and cloud backups are provided for all covered servers (and workstations, if specified) that store data or support network configurations. These endpoint backups are fully configured and automated to securely and efficiently back up your data to the cloud. When the Customer has an available local storage device, local backups are also implemented to enable faster restore times. SaaS backups for Microsoft 365 data are included for Customers subscribed to our Microsoft 365 Procurement & Tenant Configuration service only. All data is backed up and retained in accordance with the Backup Policies defined below. Restore points (date and time-specific file versions) are available strictly within the limits and guidelines of the applicable retention policy.[1]<br><br>**Backup Policy #1 — (Basic Care default)**<br>• **Retention:** 30 days<br>• **Snapshot Frequency:** Daily (1 snapshot per day)<br>• **Use Case:** Ideal for standard environments where daily restore points are sufficient and rapid rollback is not mission-critical.<br>• **Restore Options:** Files can be restored from daily snapshots taken over the previous 30 days.<br><br>**Backup Policy #2 — (Net Care default)**<br>• **Retention:** 60 days<br>• **Snapshot Frequency:** Every 4 hours (6 snapshots per day)<br>• **Use Case:** Designed for active production workloads with frequent changes and shorter recovery window requirements.<br>• **Restore Options:**<br>  ○ Restore from 4-hour interval snapshots for the most recent 30 days.<br>  ○ Restore from consolidated daily snapshots for up to 60 days.<br>  ○ Provides greater file version availability for more granular recovery.<br><br>**Backup Policy #3 — (Total Care default)**<br>• **Retention:** 60 days<br>• **Snapshot Frequency:** Hourly (24 snapshots per day)<br>• **Long-Term Snapshot:** One additional consolidated snapshot retained from 1 year prior<br>• **Use Case:** Intended for mission-critical systems requiring maximum recovery granularity and long-term rollback protection.<br>• **Restore Options:**<br>  ○ Restore from hourly snapshots for the most recent 30 days.<br>  ○ Restore from consolidated daily snapshots for up to 60 days.<br>  ○ Restore from a consolidated snapshot retained for up to 1 year.<br>  ○ Offers the highest level of file version granularity and recovery flexibility.<br><br>**Included Data Storage (all tiers are upgradable[2]):**<br>• **Basic Care:** 1TB included<br>• **Net Care:** 2TB included<br>• **Total Care:** 5TB included<br><br>[1]Data is typically backed up only from your server(s). All application data paths and user folders (e.g., “My Documents,” “Documents,” etc.) must be redirected to server-based user folders. We may initially redirect these folders for customers during the onboarding process; however, it is your responsibility to ensure users are saving all data to server folders and **not** to local workstations—including their “Desktop” or local “My Documents” folders. If you have any doubt that data is being saved to the server, you must notify us so we can verify the data paths. Unless specifically stated in the Quote, we do not back up individual workstations.<br><br>[2]Additional storage capacity can be added to any plan at any time for additional fees. |

| | |
|---|---|
| **Priority Response** | All emergency service requests shall receive a priority response in accordance with the applicable Agreement type. Non-critical service requests shall be prioritized based on the Agreement type, the nature and severity of the issue, and the requested timeframe for service. To qualify for emergency priority handling, the request must be explicitly identified as an emergency at the time of submission via telephone. If a service ticket is submitted by email and emergency handling is required, the requesting party must additionally place a telephone call and clearly identify the ticket as an emergency. Failure to provide telephone notification will result in the request being processed under standard (non-emergency) priority guidelines. |
| **Loaner Servers** | EMD maintains a dedicated pool of loaner servers to ensure business continuity in the event of a Customer's production server failure for certain Agreement levels. These loaner systems are made available on a temporary basis to restore operations while the affected production server is being repaired or replaced. This approach minimizes downtime and helps maintain service availability during unexpected hardware or system failures. |
| **3rd Party Software Patching** | Automated patching and version management for frequently used applications—such as Adobe software, Google Chrome, and other third-party tools—ensuring consistent updates, improved security, and reduced manual maintenance. |
| **Labor Rate Discounts for Out-of-Scope Work/Projects** | For any projects or issues deemed out of scope under the Customer's agreement, EMD will provide services at discounted labor rates based on the Customer's applicable agreement level. Discounts will be applied to EMD's then-current standard labor rates, as published at emdnet.com/rates. |

| LABOR-INCLUSIVE SERVICES | GENERAL DESCRIPTION |
|---|---|
| **Remediation of Detected Security Issues** | Respond to and remediate security alerts generated by EMD's security platforms, including Endpoint Detection and Response (EDR), anti-virus, anti-malware, Identity Threat Detection and Response (ITDR), and other monitoring systems. While certain threats are automatically contained or resolved through built-in automation, many alerts require manual investigation, analysis, and hands-on intervention by our technicians to fully remediate and restore systems to a secure state. This includes validating alerts, isolating affected assets when necessary, removing malicious artifacts, addressing vulnerabilities, coordinating with end users, and documenting resolution actions to ensure compliance and continuous improvement. |
| **Connectivity Problem Resolution** | Includes labor for issues related to connectivity of standard local, network and internet-connected devices. This covers servers, workstations, switches, routers, email connectivity, standard printers, and any issue that restricts normal access to the local network infrastructure or standard connected devices. Excludes proprietary or non-standard devices that are not part of the core network infrastructure. Examples include timeclocks, medical devices, devices used exclusively with proprietary software, telephones, VoIP phones, and proprietary software–related connectivity issues. This coverage does not include the cost of hardware, cabling, or replacement equipment if the connectivity issue is determined to be caused by defective hardware or physical components. Does not include labor to connect new devices, or newly added devices by Customer. |
| **Network Health Assessment** | Starting with onboarding—and continuing on a regular basis thereafter—we implement dozens of proven best practices to secure your network, enhance user productivity, and ensure your systems run smoothly. These measures include securing routers and access points; establishing strong password policies; configuring antivirus protection; verifying battery backups and data backup systems; strengthening email security; monitoring server health; optimizing firewall configurations; reviewing cabling; hardening server security; and keeping software, operating systems, and firmware up to date—among many other critical controls. Our best-practices checklist is continuously reviewed and expanded to reflect the latest technologies, threats, and industry standards, ensuring your systems remain secure, efficient, and resilient over time. Reports provided to review status and present recommended projects. |
| **Emergency After-Hours Support** | Provides after-hours labor coverage for emergency incidents that occur outside of EMD's normal business hours. Coverage applies only to true emergencies where a system required by the Customer after-hours is down or severely impaired.<br>To request after-hours emergency support, the Customer must call EMD's regular phone number during after-hours and select the Emergency options. Requests submitted via email or the customer portal will not be monitored or responded to after-hours. The number of covered emergency incidents is defined in the Quote and depends on the Customer's Agreement level (typically only Total Care includes a set number of covered incidents). Any request submitted after-hours as an emergency incident will count toward the maximum number of covered incidents, regardless of size or complexity. Incidents may range from a 10-minute password reset to a 10-hour server rebuild. |
| **Physical Cleaning of Production Servers** | Annual internal server cleaning to prevent dust-related thermal issues, maintain proper airflow, and improve overall system performance and longevity. May require downtime as production servers will need to be powered off during cleaning. Customer agrees to schedule cleaning (and potential downtime) during normal working hours. If Customer requires that the downtime be during after-hours, additional labor fees and/or overtime fees may apply. |

| | |
|---|---|
| **All Normal Daily IT Support Needs Included** | Labor is covered for standard day-to-day IT support needs, including (but not limited to) remote and onsite end-user support; user onboarding and offboarding; new workstation installation and configuration; Microsoft 365 user administration; operating system support (including patch-related issues); vendor liaison services; hardware troubleshooting and resolution (parts not included); mobile device email support; and other related IT support services.<br><br>**Labor is not covered for projects.** A project is defined as any new addition to your network environment—whether hardware or software—or any significant change to the structure, design, or configuration of your existing network. Projects typically involve planning, implementation, configuration, deployment, or migration work that goes beyond routine maintenance or standard support. All projects shall be quoted and approved prior to commencement of work. Labor shall be billed at the applicable Total Care discounted rate.<br><br>Examples of projects include, but are not limited to:<br>• Installing or deploying a new server (on-premises or virtual)<br>• Implementing a new network infrastructure component such as firewalls, switches, or wireless systems<br>• Adding or rolling out a new software application across the organization<br>• Migrating systems, data, or services to the cloud<br>• Performing major upgrades that substantially change system architecture<br>• Office relocations or network rebuilds<br>• Large-scale hardware refreshes<br>• Security redesigns or compliance-driven infrastructure changes |

| OPTIONAL SERVICES | GENERAL DESCRIPTION |
|---|---|
| **MS365 Procurement & Tenant Configuration** | This service includes license procurement, tenant-level configuration and governance to ensure your Microsoft 365 environment is secure and properly managed from day one. We implement **Identity Threat Detection & Response (ITDR)** and configure your environment for maximum security. In addition, we set up automated backups for your Exchange email, OneDrive, and SharePoint data. (A separate project quote may be required for migration to Microsoft 365). The service includes the Microsoft 365 licenses that best fit your business needs, then we also provision additional licensing necessary to deploy and manage advanced security features designed to protect your organization from modern threats.<br><br>**Additional security features include:**<br>• Identity Threat Detection & Response (ITDR)<br>• Advanced security configuration and monitoring<br>• Automatic backup of email, OneDrive, and SharePoint<br>• Email encryption options<br>• Ongoing security management and vulnerability monitoring<br><br>Because email remains the leading entry point for network breaches and ransomware attacks, these added layers of protection are strongly recommended and highly effective in reducing risk. After initial license procurement and tenant setup, user administration tasks such as adding, removing, modifying, or managing users are billable unless covered under your service agreement level (typically Total Care). |
| **Advanced Security Service** | Available as an upgrade with Net Care or Total Care, this security upgrade includes all security features in Total Care plus: Security Information & Even Management (SIEM) - helps detect, investigate, and respond to threats by collecting and analyzing security data from across your environment. Advanced DNS filtering – provides deeper inspection and allows for smarter decision-making than basic DNS blocking. This user/agent-based service is recommended for customers who have remote users and/or not behind a traditional firewall, and also provides content filtering. Domain-Based Message Authentication, Reporting & Conformance (DMARC) – provides advanced email spoofing protection. Vulnerability scanning – helps identify vulnerabilities such as outdated software, missing patches, weak passwords and exposed services so we can remediate them before attackers can exploit them. Support for third-party industry-specific security frameworks and associated documentation, including security audits, SOC 2, NIST, and HIPAA, to the extent the Customer is obligated to comply with these standards.<br>This level of advanced security requires all users to have MS365 Premium licenses as well as a business class router with active subscription. |
| **Advanced Backup/Disaster/Recovery (BDR) Appliance** | Backup/Disaster/Recovery (BDR) solutions significantly improve Recovery Time Objectives (RTO) by maintaining a fully redundant backup server that is continuously updated and ready to assume production workloads in the event of a system failure. This enables near-seamless failover, ensuring high availability and stronger operational resilience. A BDR works by continually restoring the most current backups onto a standby system. If the production server fails, the BDR can be brought online as the replacement server—often within minutes—rather than requiring hours or even days to replace hardware and perform a full restore. If a BDR is purchased (or already owned), EMD will manage and maintain the device to ensure it remains ready for immediate use in the event of an outage. The use of a BDR can dramatically reduce downtime compared to the traditional approach of sourcing replacement hardware and restoring data to a new or loaner server.<br>Even when EMD provides a loaner server under an agreement option, restoration time can still be significant depending on the amount of data and system complexity. If the BDR option is declined, the client will be required to purchase an external hard drive of sufficient capacity to support local backup storage. |

| | |
|---|---|
| **Password/Credential & Document Manager** | **Secure Password & Credential Management**<br>• Central **password vault** where users can safely store login credentials instead of insecure methods (like spreadsheets or sticky notes).<br>• Features include **strong password generation**, permission-based access, and encrypted storage.<br><br>**Centralized Documentation**<br>• Store and manage **standard operating procedures (SOPs)**, training materials, onboarding docs, and other organizational documents in one place.<br>• Full-text search and structured document storage help teams find what they need fast.<br><br>**Collaboration Tools**<br>• Facilitates **secure sharing** of passwords and documentation among team members and between departments.<br>• Helps organizations collaborate internally and with MSP partners via a unified portal.<br><br>**Self-Service & End-User Access**<br>• End users can **self-serve** for password resets and basic troubleshooting using shared read-only SOPs and help content, reducing support tickets.<br><br>**Mobile & Browser Extensions**<br>• Access from iOS, Android, and via browser extensions for password retrieval on the go.<br><br>**Security & Compliance**<br>• Built on a **SOC 2 / SOC 2 Type 2 compliant** platform, helping enforce secure data management practices.<br>• Role-based access controls and audit trails for tracking access and changes. |
| **EMD Phishbait** | A Security Awareness Training (SAT) program designed to educate and test users on secure email practices to help keep your network protected. This service strengthens email security by evaluating employee behavior—since the most common way viruses and ransomware enter a network is through unsafe email habits. EMD will test users through harmless simulated email campaigns designed to measure their ability to recognize and avoid phishing attempts, malicious links, and other common threats. Following the initial campaign, detailed reports will be provided identifying which users may be placing the network at risk. Based on the results, EMD will assign targeted security awareness training and follow-up testing to improve employee knowledge and reinforce safe email practices. Quarterly follow-up campaigns will then be conducted to track progress and identify any users who continue to demonstrate risky behavior. Once this service is active, EMD will not provide advance notice of phishing simulation campaigns. Notifications and reporting will be provided only after each campaign is completed. This service requires a minimum commitment of one (1) year. |

| | |
|---|---|
| **Privileged Access Management (PAM)** | Our Privileged Access Management (PAM) solution strengthens your network security by removing local administrator rights and implementing endpoint privilege management. This is one of the most effective ways to reduce your organization's attack surface. By limiting administrative privileges, PAM helps prevent malware infections and significantly reduces opportunities for attackers to exploit vulnerabilities. In addition to blocking malicious software, PAM also helps enforce company policies by preventing users from installing unauthorized or non-productive applications (such as games or other unapproved software). When an application requires administrative rights to install, PAM first checks it against your organization's pre-approved application list.<br>• If the application is approved, installation proceeds.<br>• If it is not on the approved list, we are alerted immediately. We will either approve the application (if it is safe and business-related) or consult with your management team if there is any uncertainty.<br>During normal EMD business hours, approval for safe and necessary business applications typically takes less than one minute. If a determination cannot be made within that timeframe, the installation will be placed on hold until we can review it with your management. Industry estimates indicate that operating users with standard (non-administrative) privileges can mitigate 94% or more of Microsoft-related vulnerabilities—making privilege management one of the most impactful security controls you can implement. |
| **Extended Device Management** | Centralized management of cloud-connected and mobile endpoints—including PCs, smartphones, and tablets—to enforce security standards, ensure timely patching, and maintain compliance. Provides visibility and control over extended device usage through policy-based governance, helping reduce risk, prevent unauthorized access, and support regulatory compliance across all managed devices. |
| **IP Camera Support** | Includes troubleshooting and resolution of issues related to existing IP cameras connected to the Customer's network at designated Customer locations. Services include:<br>• Diagnosing and resolving network connectivity issues<br>• Troubleshooting mobile application access and functionality problems<br>• Performing firmware updates and software maintenance as needed<br>• Managing user access changes (adding, removing, or modifying users and permissions)<br>• Configuration and setup of new replacement IP cameras (excluding physical installation or mounting)<br>• Reconfiguration or optimization of existing camera settings<br>• System diagnostics and problem identification to restore proper operation<br>This service does not include hardware replacement, physical installation, on-site cabling, or the resolution of issues outside the supported scope. This service also does not include real-time monitoring of camera footage or camera functionality. The Customer is responsible for monitoring camera footage and functionality, and for reporting any issues or camera failures to EMD. Once an issue is reported, EMD will diagnose the problem and provide a remediation plan. |
| **Two Factor Authentication** | ***Provides for additional security and access control using:***<br>• Advanced two factor authentication with advanced admin features.<br>• Secures on-premises and cloud-based applications.<br>• Permits custom access policies based on role, device, location.<br>• Identifies and verifies device health to detect "risky" devices |

| | |
|---|---|
| **VoIP Support (3rd party VoIP systems)** | **VoIP Administration & Maintenance — Included Services**<br>EMD will perform routine VoIP system administration and operational support, including but not limited to:<br>• Adding, removing, and modifying users, extensions, and associated devices<br>• Standard phone and device provisioning, including assigning/reassigning endpoints<br>• Voicemail configuration and administration (mailbox setup, your recorded greetings, password resets, and PIN changes)<br>• Configuration and maintenance of call routing features including call paths, auto attendants, hunt groups, ring groups, and related standard call flows<br>• Moves, adds, and changes (MAC) of phones within the organization, including relocation and reassignment<br>• Name changes, password resets, and other standard user/account maintenance<br>• Troubleshooting and resolution of routine configuration and functionality issues<br>• Coordination with telecommunications carriers, hosted VoIP providers, and other communication vendors to resolve service-affecting issues<br>• Performing firmware updates for supported devices when required<br>• Applying routine software updates/patches as needed to maintain security and system stability<br><br>**Exclusions -** The following services are explicitly excluded from this scope and may require a separate project engagement, or additional fees:<br>• Hardware replacement, physical repair, or onsite break/fix services<br>• Complete reinstallation, rebuild, or full migration of the VoIP system (considered a project)<br>• Call quality issues not attributable to the internal network (e.g., ISP, carrier, or upstream provider issues), except for vendor coordination as described above<br>• Business hours changes or schedules management (except for annually)<br>• Rollover deployments or large-scale phone rollouts beyond routine adds/moves/changes<br>• Creation, editing, or deployment of custom call recordings (including professional voice recordings)<br>• Support for end-of-life (EOL) hardware, unsupported platforms, or deprecated firmware/software versions |
| **Managed DMARC** | Helps prevent email and domain spoofing by strengthening authentication protocols and protecting your brand from impersonation attacks. This can prevent reputation damage and potential abuse or blacklisting issues. The price quoted covers one domain; additional domains can be added for an extra monthly fee. |
| **Remote Access** | Enables secure remote access to a user's work computer, allowing them to log in and operate their physical workstation from an offsite location. Requires a dedicated physical device installed onsite to support the remote connection. |

| | |
|---|---|
| **EMD VoIP** | EMD VoIP (Voice over IP) provides hosted PBX, VoIP, SIP Trunking, and Unified Communications. These services include cloud-based voice solutions with full PBX functionality and enterprise-grade features. VoIP features may include, but are not limited to: virtual auto attendant, voicemail-to-email, call forwarding/follow-me, conference calling, direct inward dialing (DID), call transfer, call parking, and other standard PBX call management features.<br><br>Our VoIP services..<br>• Are not dependent on any specific internet provider<br>• May be used with desk phones, mobile phones, or softphone applications<br>• Provide high-quality, reliable cloud-based communications<br>• Include an easy-to-use management interface<br>• Offer modern PBX functionality with scalable enterprise capabilities<br>• Typically reduce upfront and long-term costs compared to traditional on-premise phone systems<br>• **Include <u>local</u> service and support** |
| **Workforce Productivity** | Workforce analytics platform that transforms digital work activity data into actionable insights to improve productivity and performance—whether teams are in-office or remote. Provides a complete view of work patterns, productivity trends, and potential blockers, enabling agile, data-driven decision-making. Organizations can optimize technology usage, streamline workflows, support performance coaching, and share meaningful weekly insights with managers and employees—all while maintaining strong data privacy and security standards.<br><br>**Key Capabilities:**<br>• Workforce & Remote Workforce Management<br>• Employee Monitoring & Time Tracking<br>• Productivity & Performance Optimization<br>• Workforce Planning & Capacity Management<br>• Technology & Office Space Optimization<br>• Schedule Compliance & Contractor Billing Reconciliation<br><br>Empowers organizations to quickly optimize performance, reduce costs, and drive sustainable productivity growth. |
| **Managed Email Signatures** | Managed email signature service for centrally creating and managing email signatures, legal disclaimers and more across your entire Microsoft 365 organization. Works seamlessly with **all email apps and devices** — including Windows, Mac, mobile phones, and tablets.<br><br>**Key benefits:**<br>• Centralized management of company-wide email signatures and branding<br>• Automatically applies consistent signatures to emails sent from any email client or device<br>• Enables fully branded signature designs, with different versions for **new messages** and **replies/forwards** |

## Covered Equipment / Hardware / Software

Managed Services will be applied to the equipment listed in the Quote ("Covered Hardware"). If specific equipment including serial numbers can not be listed at the time of the Quote, the quantities on the Quote will be used for billing and an inventory of the equipment will be performed during on-boarding. All servers and workstations that are connected to the network, physically or remotely, must be covered.

We will facilitate support for software on managed devices ("Supported Software"); provided, however, all Supported Software must, at all times, be properly licensed and under a maintenance and support agreement from the Supported Software's manufacturer. In this Services Guide, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

## Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Onsite visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Customer's primary office location listed in the Quote. Fees charged for locations include monitoring of that location's switches, routers, access points and application of EMD's security stack for protection. Labor to resolve issues with these devices and services are covered only if the plan you select includes labor for the specific service needed. Cabling within walls, ceilings or other enclosures is not covered. If there is no physical location, this fee covers the same for problems with connectivity to the cloud/remote computers and the switches/routers between those connections.

# Term; Termination

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to EMD's satisfaction.

The Services will continue through the Initial Term, and then on a monthly basis, until terminated as provided in the Agreement, the Quote, or as indicated in this section (the "Service Term").

**Auto-Renewal**. After the Initial Term, the Services will continue to be billed automatically each month. Either party may terminate the Service Term at any time by providing the other party with no less than thirty (30) days prior written notice.

**Per Seat Licensing**: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat licenses (such as, if applicable, Microsoft NCE licenses) that we acquire on your behalf. Please see "Per Seat License Fees" in the Fees section below for more details.**

# Assumptions / Minimum Requirements / Exclusions

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements:

- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software, or if our Services begin prior to you licensing supported versions of Microsoft Windows®, then you agree that within 90 days after Services begin, you will update to a current version on the Covered Hardware or replace the applicable devices with equipment that comply with this paragraph.
- All software must be genuine, licensed and vendor-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The Environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the environment must be securely encrypted.
- An outside static IP address may be required for some remote access solutions and we highly recommend one for those types of services.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Customer must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Customer must provide us with exclusive administrative privileges to the Environment.
- Customer must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

***Exclusions***. Services that are not expressly described in the Quote will be out of scope and will not be provided to Customer unless otherwise agreed, in writing, by EMD. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by EMD in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the Environment up to the Minimum Requirements (unless otherwise noted in “Scope of Services” above).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

# Service Levels

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-TH, 8AM–5PM, FRI 7AM–4PM Pacific Time, excluding legal holidays and EMD-observed holidays (listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

**If the Quote indicates that you receive our Total Care Service**: We will respond to emergency or critical issues (defined as situations in which all or practically all of an entire managed network is affected) within two (2) business hours after being notified of the applicable issue*; all other issues will be provided on a "best efforts" basis and are subject to technician availability.

**If the Quote indicates that you receive our Net Care Service**: We will respond to emergency or critical issues (defined as situations in which all or practically all of an entire managed network is affected) within four (4) business hours after being notified of the applicable issue*; all other issues will be provided on a "best efforts" basis and are subject to technician availability.

> ** All time frames for emergency/critical response are calculated as of the time that EMD is notified of the applicable issue / problem by Customer by telephone at the telephone number listed in the Quote to our dispatcher. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts. Emailing or calling a technician directly is not acceptable and will cause delays in our response.*

Technical support under any service plans other than Total Care and Net Care will be provided on a "best efforts" basis and are subject to technician availability.

**Support During Off-Hours/Non-Business Hours**: If the Quote indicates that you receive our Total Care Service: You will receive support for up to two (2) incidents per month requiring after-hours support.

Technical support provided outside of our normal business hours (other than indicated above) are offered on a case-by-case basis, and are subject to technician availability. If EMD agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then the support will be provided on a time and materials basis (which unless specifically stated, is not covered under any Service plan), and will be billed to Customer at our then-current overtime rates.

All hourly services are billed in 15 minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

**EMD-Observed Holidays**: EMD is closed for the following holidays, if they fall on a regular work day. If they fall on a non-work day they may be 'observed' on a day other than the date of the holiday:

- New Year's Day
- Good Friday – Half Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve

- Christmas Day
- New Year's Day

**Service Credits**: Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Customer timely brings that failure to our attention in writing (as per the requirements of the MSA), then Customer will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

## Auditing Services

We will audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services are comprised of:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software
- Security vulnerability check
- Backup and disaster recovery solution audit
- Speed test and ISP audit
- Office phone vendor service audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

# On-boarding Services

If onboarding services are provided under the Quote, then the following services will be provided to you.

- Secure network by changing passwords for admins, user accounts, routers, switches, email accounts, ILO access, VPN's, etc. using secure password formats.
- Uninstall any monitoring tools or other software installed by previous IT consultants.
- Determine existing backup strategy and status; prepare backup options for consideration and get backups scheduled asap.
- Redirect local folders so data gets saved to proper locations to be backed up.
- If the Quote includes Managed Email, prepare and schedule backups of MS365 accounts asap.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous virus protection and RMM agents and install our managed antivirus application and RMM agents.
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup, antivirus, and spyware scans.
- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on all devices.
- Stabilize network and assure that all devices can securely access the file server.
- Review and document current server configuration and status.
- Review password policies and update user and device passwords.
- Review group policy settings and make changes as needed.
- Review and setup printers properly for best practices.
- Gather and document all SSL certs, domains and other registrations to manage renewals.
- Distribute instructions on requesting service, dispatch guidelines, etc to end users.
- As applicable, make recommendations for changes that should be considered to the managed environment.
- More (over 90 total items in our complete on-boarding task list)

The foregoing list is subject to change if we determine, in our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.

# Ongoing / Recurring Services

Ongoing/recurring services are services that are provided to you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Ongoing services generally begin upon the completion of on-boarding services; therefore, any delays or interruptions to the onboarding services may delay the commencement of ongoing/recurring services.

# Fees

The fees for the Services will be as indicated in the Quote.

*Changes to Environment*. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of supported devices in the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

*Minimum Monthly Fees*. The initial Fees indicated in Quote are the minimum monthly fees ("MMF") that will be charged to you during the term. You agree that the amounts paid by you under the Quote will not drop below the MMF regardless of the number of users or devices to which the Services are directed or applied, unless we agree to or initiate the reduction. We will perform periodical assessments of the number of devices and users to determine if the fees should be increased or decreased based on any quantity changes.

*Increases*. In addition, we reserve the right to increase our monthly recurring fees and, if applicable, our data recovery-related fees; provided, however, if an increase is more than five percent (5%) of the fees charged for the Services in the prior calendar year, then you will be provided with a sixty (60) day opportunity to terminate the Services by providing us with written notice of termination. You will be responsible for the payment of all fees that accrue up to the termination date and all pre-approved, non-mitigatable expenses that we incurred in our provision of the Services through the date of termination. Your continued acceptance or use of the Services after this sixty (60) day period will indicate your acceptance of the increased fees.

In addition to the foregoing, we reserve the right to pass through to you any increases in the costs and/or fees charged by third party providers for the third party services ("Pass Through Increases"). Since we do not control third party providers, we cannot predict whether such price increases will occur, however, should they occur, we will endeavor to provide you with as much advance notice as reasonably possible.

*Travel Time*. If onsite services are provided, we will travel to locations within city limits at no charge. Time spent traveling outside city limits will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you. If you have a current Net Care or Total Care agreement, all onsite travel will be at no charge unless you request additional onsite visits that are not required for the normal servicing of your account under the agreement.

*Appointment Cancellations*. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

*Automated Payment*. You may pay your invoices by check and/or by ACH, as described below. For all recurring services we require "Auto-pay" by way of ACH through our payment portal at

portal.emdnet.com. We only accept payment by credit card for non-recurring fees/invoices that are under $1,000. All invoices over $1,000 for recurring fees and non-recurring fees may not be paid by credit card.

- **ACH**. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions. All monthly fees for recurring agreements must be paid via ACH.
- **Credit Card**. When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote. We do NOT allow invoices over $1,000 to be paid by credit card. These invoices must be paid either by ACH or check. All monthly fees for recurring agreements must be paid via ACH and are not to be paid with a credit card.
- **Check.** You may pay by check provided that your check is delivered to us prior to the commencement of Services. Checks that are returned to us as incorrect, incomplete, or "not sufficient funds" will be subject to a $50 administration fee and any applicable fees charged to us by your bank or financial institution.

*Microsoft Licensing Fees*. The Services require that we purchase certain "per seat" licenses from Microsoft (which Microsoft refers to as New Commerce Experience or "NCE Licenses") in order to provide you with one or more of the following applications: Microsoft 365, Dynamics 365, Windows 365, and Microsoft Power Platform (each, an "NCE Application"). **As per Microsoft's requirements, NCE Licenses cannot be canceled once they are purchased and cannot be transferred to any other customer. Each NCE License that we purchase may require a one (1) or three (3) year term. For that reason, you understand and agree that regardless of the reason for termination of the Services, you are required to pay for all applicable NCE Licenses in full for the entire term of those licenses.** Provided that you have paid for the NCE Licenses in full, you will be permitted to use those licenses until they expire, even if you move to a different managed service provider.

*Labor Rate Discounts*. For projects or issues that are 'out of scope' of the customer's agreement, labor discounts are offered as indicated on your agreement. Discount is for any work done for the customer that is not covered by their agreement. These discounts are offered off our regular labor fees which are subject to change at any time. You can view our current labor rates at https://emdnet.com/rates.

## Requesting Service

When requesting service, it is important to follow these guidelines to obtain the fastest response and to alert the proper departments/individuals. Always request service in one of the following ways only:

- **Preferred and fastest method** - Email help@emdnet.com with a brief description of the issue in the subject line and details of the issue in the body of the email. Include anything you feel will be helpful for us to schedule the right resource and so that resource can be properly prepared to resolve the issue. This will get a ticket created immediately and put into our service queue.
- Call one of our main phone lines at 559-636-7000 or 805-439-1055 and follow the prompts to request service.
- Use our customer portal at portal.emdnet.com to create a new ticket.

**Do not contact a technician** or other EMD employee directly to request service as this will only delay the response and may not get scheduled for an extended period of time. Our technicians are not allowed to schedule themselves, nor do they have the resources to do so. They also may not receive your email or voice message for an extended period of time, therefore delaying the service unnecessarily.

**For emergency service requests** always call one of our main phone lines and indicate to the dispatcher that it is an emergency request. Emergency requests should be limited to situations where all or the majority of your Environment is down or severely limited.

**For after hours service requests** call one of our main phone lines and follow the prompts. Someone will contact you as soon as possible. Unless your agreement includes after hours support, you will be charged our normal overtime rates with a minimum charge of 1 hour.

## Removal of Software Agents

Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the Environment. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the Environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, Customer will remove, package and ship, at Customer's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Customer by EMD that were used in the provision of the Services. If you fail to timely return all equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

# Additional Terms

**Authenticity**

Everything in the managed environment must be genuine and licensed—including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

**Monitoring Services; Alert Services**

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by EMD, and Customer shall not modify these levels without our prior written consent.

**Remediation**

Unless otherwise provided in the Quote, remediation services will be provided in accordance with the recommended practices of the managed services industry. Customer understands and agrees that remediation services are not intended to be, and will not be, a warranty or guarantee of the functionality of the Environment, or a service plan for the repair of any particular piece of managed hardware or software.

**Configuration of Third Party Services**

Certain third party services provided to you under this Services Guide may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without our knowledge or authorization could disrupt the Services and/or or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

**Modification of Environment**

Changes made to the Environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the Environment without our prior knowledge or consent. For example, you agree to refrain from adding or removing hardware from the Environment, installing applications on the Environment, or modifying the configuration or log files of the Environment without our prior knowledge or consent.

**Co-Managed Environment**

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by us), we will endeavor to implement the Services an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed

Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention.

**Anti-Virus; Anti-Malware**

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. In order to improve security awareness, you agree that EMD or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

**Breach/Cyber Security Incident Recovery**

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data impacted by the incident will be recoverable. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Customer's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the Environment, or (ii) prevents normal access to the Environment, or impedes or disrupts the normal functions of the Environment.

**Environmental Factors**

Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances.

**Fair Usage Policy**

Our Fair Usage Policy ("FUP") applies to all Services that are described or designated as "unlimited." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating

urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

**Hosted Email**

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email"). Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by EMD or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. EMD reserves the right, but not the obligation, to suspend Customer's access to the Hosted Email and/or all transactions occurring under Customer's Hosted Email account(s) if EMD believes, in its discretion, that Customer's email account(s) is/are being used in an improper or illegal manner.

**Patch Management**

We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.

**Backup (BDR) Services**

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Customer's data. Neither EMD nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. EMD cannot and does not warrant that data corruption or loss will be avoided, and Customer agrees that EMD shall be held harmless if such data corruption or loss occurs. Customer **is**

**strongly advised to keep a local backup of all of stored data to mitigate against the unintentional loss of data.**

**Procurement**

Equipment and software procured by EMD on Customer's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Customer to the greatest extent possible. By procuring equipment or software for Customer, EMD does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Customer's responsibility in the event that a return of the Procured Equipment is requested. EMD is not a warranty service or repair center. EMD will facilitate the return or warranty repair of Procured Equipment; however, Customer understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which EMD will be held harmless, and (ii) EMD is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier. If equipment is purchased through EMD, we will handle the processing of any warranty claims, shipping the product back to the vendor (if applicable) and receiving the product back from the vendor and testing before putting it back into the Environment. Because of this service, EMD may not be able to match or be comparable to pricing you may be able to obtain elsewhere or on your own. If equipment is purchased by you directly (not through EMD) you will be responsible for the processing of any warranty claims, shipping the product and receiving it and testing before it is put back into the Environment.

**Best Practice Reviews/Heath Assessments; IT Strategic Planning**

Suggestions and advice rendered to Customer are provided in accordance with relevant industry practices, based on Customer's specific needs and EMD's opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, EMD is not endorsing any particular manufacturer or service provider.

**Penetration Testing; Vulnerability Assessment**

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing process, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees or expenses arising or resulting from (i) any response to the penetration testing services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

**No Third Party Scanning**

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or

solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity is not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

**Obsolescence**

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires "end of support" status from the applicable device's or software's manufacturer ("Obsolete Element"), then we may designate the device or software as "unsupported" or "non-standard" and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our "best efforts" only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element, (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose), or (iii) remove the Obsolete Element from the Environment so it does not risk the security of the rest of the Environment. If you are not agreeable to any of these options we may elect to cancel Services to avoid risk or liability of the Environment's security. In any event, we make no representation or warranty whatsoever regarding any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

**Hosting Services**

You agree that you are responsible for the actions and behaviors of your users of the Services. In addition, you agree that neither Customer, nor any of your employees or designated representatives, will use the Services in a manner that violates the laws, regulations, ordinances, or other such requirements of any jurisdiction.

In addition, Customer agrees that neither it, nor any of its employees or designated representatives, will: transmit any unsolicited commercial or bulk email, will not engage in any activity known or considered to be "spamming" and carry out any "denial of service" attacks on any other website or Internet service; infringe on any copyright, trademark, patent, trade secret, or other proprietary rights of any third party; collect, attempt to collect, publicize, or otherwise disclose personally identifiable information of any person or entity without their express consent (which may be through the person or entity's registration and/or subscription to Customer's services, in which case Customer must provide a privacy policy which discloses any and all uses of information that you collect) or as otherwise required by law; or, undertake any action which is harmful or potentially harmful to EMD or its infrastructure.

Customer is solely responsible for ensuring that its login information is utilized only by Customer and Customer's authorized users and agents. Customer's responsibility includes ensuring the secrecy and strength of user identifications and passwords. EMD shall have no liability resulting from the unauthorized use of Customer's login information. If login information is lost, stolen, or used by unauthorized parties or if Customer believes that any hosted applications or hosted data has been accessed by unauthorized parties, it is Customer's responsibility to notify EMD immediately to request the login information be reset or unauthorized access otherwise be prevented. EMD will use commercially reasonable efforts to implement such requests as soon as practicable after receipt of notice.

**Licenses**

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.