datanetworks

v11-4-25

MSP Services Guide

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the quote that has been provided to you (the "Quote"), as well as the policies and procedures that we follow (and to which you agree) when we provide a service to you or facilitate a service for you. If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Data Networks of America, Inc. ("Data Networks," "we," "us," or "our"); **however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").**

This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

Please read this Services Guide carefully and keep a copy for your records.

Last Updated: November 2025

1. Onboarding Services

Onboarding is accomplished in two phases. Phase 1 is to assess your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. We evaluate the current state of your IT infrastructure, systems, processes, and overall technology environment. This assessment is crucial to gather critical information, identify potential areas for improvement, and develop a plan for delivering our managed services effectively. Our assessment includes some or all the following:

a. Introduction
    i. Introduce the Data Networks team and explain the purpose of the assessment.

b. IT Policy Review
    i. Review your existing policies and provide recommendations for the creation of additional standard IT policies related to the use of your technology.

ii. Gap Analysis: Conduct an analysis to identify gaps between current policies and best practices, including security, data protection, acceptable use, and disaster recovery. This analysis is limited to standard, common IT policies.
    1. Please Note: The creation, development, and implementation of new policies is available via a separate Professional Services engagement.

c. Infrastructure and Network Assessment
    i. Asset Inventory: Document existing hardware, including servers, workstations, network devices, and peripherals.
    ii. Network Topology: Map the current network topology, including routers, switches, firewalls, and wireless networks.
    iii. Bandwidth and Performance: Evaluate network bandwidth, latency, and overall performance.

d. System and Application Assessment
    i. Software Inventory: Compile a list of installed software applications and versions on servers and workstations.
    ii. Critical Applications: Identify mission-critical applications and their dependencies.

e. Security Review
    i. User Access Controls: Evaluate user access controls, permissions, and authentication methods.
    ii. Endpoint Security: Assess antivirus, anti-malware, and endpoint protection solutions.
    iii. Firewall Configuration: Review firewall configurations and rules.
    iv. Data Encryption: Check for data encryption mechanisms, especially as relates to sensitive information.

f. Data and Backup Assessment
    i. Data Storage: Evaluate current data storage solutions and capacity.
    ii. Backup and Recovery: Review current backup strategies, frequency, and recovery procedures.
    iii. Disaster Recovery Plan: Confirm whether a disaster recovery plan is in place.

g. Cloud and Virtualization Assessment
    i. Cloud Services: Identify and assess the use of cloud services.
    ii. Virtualization: Evaluate virtualization technologies in use.

h. Vendor and Licensing Assessment
    i. Vendor Relationships: Review and understand current relationships with technology vendors and service providers.
    ii. Licensing Review: Determine the legality and cost-effectiveness of software licenses.

i. Documentation Review
    i. Document Review: Collect and review existing documentation related to IT infrastructure, systems, policies, and procedures.
    ii. Documentation Quality: Assess the quality and completeness of existing documentation.

If deficiencies are discovered during the assessment process (such as outdated equipment or unlicensed software), we will bring those issues to your attention, discuss the impact of the deficiencies on our provision of Services, and provide you with options to correct the deficiencies.

Please Note: unless otherwise expressly agreed by us in writing, assessment 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 assessment process. Issues that are discovered in the Environment after the assessment process is completed may be addressed in one or more subsequent quotes.

Phase 2 of onboarding is to prepare your IT environment for the monthly managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) to review the information we need to prepare the targeted environment. This includes:

j. Initial Consultation
    i. Conduct a consultation meeting to review the findings of the initial assessment and next steps in the onboarding process.
    ii. Secure admin access for domain and global admin accounts.

k. RMM Agents
    i. Provide and install remote connection node.
    ii. Deploy RMM agents to all endpoints and devices for ongoing monitoring, management, and support.
    iii. Configure RMM tools for automated alerts, patch management, and remote assistance.

l. EDR and Managed SOC Solutions
    i. Install EDR agents on endpoints to detect, investigate, and respond to threats.
    ii. Implement Managed SOC services for advanced threat monitoring, detection, and response capabilities, leveraging both technology and expert analysis.

m. Network Security Enhancements
    i. Deploy the standard firewall solution and configure settings tailored to your specific security needs.

n. Data Protection and Backup
    i. Set up data backup solutions, schedule regular backups, and establish disaster recovery protocols.
    ii. Ensure encryption is in place for sensitive data, both at rest and in transit.

o. Documentation and Compliance
   i. Create comprehensive documentation of your IT infrastructure, configurations, and procedures.
   ii. Ensure compliance with relevant industry regulations and standards.

p. Training and Access Management
   i. Provide training sessions on cybersecurity best practices and how to use new systems or software.
   ii. Set up user accounts, permissions, and access controls, ensuring secure authentication methods are in place.

q. Final Onboarding Review
   i. Conduct a final onboarding review meeting with you to ensure all systems are operational and to address any questions.
   ii. Provide You with contact information for support and account management.
   iii. Engage end users with introductory support materials.
   iv. Schedule reoccurring cadence for TAM and Strategic Alignment meetings.
   v. Review and adjust server, user backup settings, and security configurations.
   vi. Audit and update alert notification and documentation settings.

Please Note: This list is subject to change if we determine, at our discretion, that different or additional onboarding activities are required. The duration of the onboarding process depends on a number of factors, many of which may be outside of our control - such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

2. Recurring Services – Base Services

Ongoing/recurring services are services that are provided to you or facilitated for you on a 10% ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or "go live" dates to your account manager.

a. **Advanced Endpoint Detection and Response (EDR)**
   Implementation and facilitation of an endpoint malware and advanced threat protection solution utilizing an Endpoint Detection and Response (EDR) solution from our designated Third-Party Provider.
   i. Real-Time Threat Detection: EDR solution continuously monitors endpoints for suspicious activities. Using advanced algorithms and machine learning, it identifies potential threats in real-time, ensuring immediate response to any security incidents.

ii. Automated Response Capabilities: Upon detecting a threat, the system automatically initiates a response. This may include isolating the affected endpoint, removing malicious files, or reversing unauthorized changes, thereby minimizing the impact on your operations.
iii. Behavioral AI Technology: Utilizing behavioral AI technology which goes beyond traditional signature-based approaches, it analyzes patterns and behaviors, enabling it to detect and block even the most sophisticated, previously unknown threats.
iv. 24/7 Monitoring: EDR solution provides round-the-clock monitoring. We ensure that any alerts are investigated and resolved.
v. Comprehensive Reporting and Analytics: Provide detailed reports and analytics, giving you insights into the security landscape of your endpoints. This includes information on detected threats, response actions taken, and recommendations for enhancing your security posture.

b. **Attack Surface Management (Unified IT Documentation and Automation Platform)**
We use an automated IT documentation and intelligence platform to give you complete visibility into your technology environment. It continuously collects configuration data from your cloud services, servers, network devices, and applications so that everything stays accurate, monitored, and aligned with best practices.
i. Always up to date: Your systems are automatically documented and refreshed with the latest configuration data, so there's no risk of outdated or missing information.
ii. Proactive insight: We can quickly detect and address unauthorized or risky changes before they cause downtime or security issues.
iii. Better compliance: Detailed configuration tracking supports audit readiness for frameworks such as CIS.
iv. Faster resolution: When issues arise, our engineers have instant access to accurate system data, which speeds up troubleshooting and reduces disruption.
v. Smarter planning: With a clear picture of your environment, we can identify trends, forecast needs, and help you make informed IT decisions.

c. **Asset Inventory and Management**
Implementation and management of our Asset Inventory and Management solution for efficiently managing all your IT assets. This service enables tracking of hardware, software, and other IT resources, to help ensure optimal utilization and management throughout their lifecycle.
i. Comprehensive Asset Tracking: Asset and Inventory Management tool maintains a detailed inventory of all IT assets. This includes hardware devices, software licenses, network equipment, and any other technology infrastructure managed under this contract.

ii. Real-Time Documentation: Provide dynamic, real-time documentation of your IT environment. This ensures that the information about your assets is always up-to-date, accurate, and readily available.
iii. Automated Asset Discovery: The service includes automated discovery of new and existing assets within your network. This feature ensures that all assets are accounted for and properly documented without manual intervention.
iv. Centralized Information Repository: Our Asset Inventory and Management tool serves as a centralized platform for all asset-related information. This includes purchase details, warranty information, configuration settings, and associated documentation.
v. Lifecycle Management: We assist in managing the entire lifecycle of your assets, from procurement and deployment to maintenance and eventual decommissioning or replacement.

d. **Disc Encryption for Windows and Mac**
Provides full disk encryption, enhancing the security of the data stored on the Windows operating system drive and additional data drives. Encrypts the entire contents of a disk drive, including the operating system, system files, and user data. This ensures protection of the data from unauthorized access even if the physical drive is removed and connected to another system.

e. **Feature Updates for Workstations**
Managing feature updates, particularly for operating systems like Windows, is an essential part of maintaining a secure and up-to-date IT environment. Please Note: This service is scheduled annually.
i. Communicate with stakeholders, including end-users, IT staff, and management, about the upcoming feature update. Provide a clear plan outlining the timing, impact, and benefits of the update.
ii. Before initiating the feature update, ensure that the workstation has been backed up.
iii. Provide rollback plan and mechanism in case any issues arise during or after the update.
iv. Coordinate with you to schedule the upgrade to minimize disruption during the feature update process. Where possible, implement the update during non-business hours to minimize the impact to end users.
v. Configure automated deployment policies within our RMM tool to manage the rollout of feature updates.
vi. Monitor the progress of feature update deployments. Generate post-update status reports.
vii. Provide you with instructions on what to expect, any required actions, and who to contact in case of issues.

f. **Firewall Management (firewall appliance provided/purchased by Client)**
An effective firewall prevents unauthorized users from accessing internal network(s) from outside the network(s), provides secure and encrypted remote network access;

provides antivirus scanning for all traffic entering and leaving the managed network; and provides website content filtering functionality.

i. Provide an initial review of the configuration of the firewall against best practices. Make appropriate changes, if applicable.
ii. Monitor, update (software/firmware), and support Client-supplied firewall appliance.

g. **Firmware Updates**

We handle firmware updates through our RMM tool which supports firmware management for a variety of devices and provides a centralized interface for monitoring, scheduling, and deploying firmware updates. We follow a systematic approach, as firmware updates are critical to maintain the security and performance of hardware components.

i. Regularly check the websites or documentation of hardware vendors for firmware updates. Vendors often release updates to address security vulnerabilities, enhance features, or improve performance.
ii. Prioritize firmware updates based on criticality and security impact. Schedule updates during maintenance windows or periods of low activity to minimize disruption.
iii. Before applying firmware updates, perform backups of configurations and settings. Provide a well-defined rollback plan in case an update causes issues, allowing for a quick return to the previous firmware version.
iv. Configure automated scanning through the RMM tool to identify devices with outdated firmware versions. Regularly scan the network to ensure that all devices are up to date.
v. Enable monitoring features to track the progress of firmware updates. Configure alerts to notify administrators of any failed updates or potential issues during the deployment.

h. **Managed Identity Threat Detection and Response**

We use a managed detection and response platform to help protect your systems from advanced cybersecurity threats that traditional antivirus tools often miss. It provides continuous monitoring, threat detection, and expert-led response to help keep your business safe from evolving cyberattacks.

i. Continuous Monitoring and Surveillance: Your environment is monitored around the clock to identify potential security incidents before they escalate, ensuring real-time awareness and faster response.
ii. Advanced Threat Detection: A combination of cutting-edge technology and human expertise helps identify everything from common malware to sophisticated attacks. This proactive approach reduces the likelihood of significant damage or downtime.
iii. Incident Response and Management: When a security incident occurs, our team responds quickly to contain the threat, eliminate malicious activity, and restore normal operations with minimal impact to your business.

iv. Expert Analysis and Investigation: Each alert is reviewed by a cybersecurity team who investigate root causes, assess impact, and recommend preventative measures to strengthen your defenses.
v. Compliance and Reporting: You'll receive regular reports that outline detected threats, response actions, and overall security trends—helping you maintain compliance with regulatory standards and improve your long-term security posture.
vi. Seamless Integration: The service integrates directly with your existing IT systems, adding an extra layer of protection without disrupting operations.
vii. Incident Response Guide: All activity follows our Managed Incident Response Guide, ensuring consistent, structured, and timely response procedures.

i. **Microsoft File and Email Encryption Labels**
System changes for automatic encryption to help ensure the confidentiality of sensitive information; enables ability to flag sensitive information (MS Office labels) to automatically encrypt data. Please Note: Microsoft Business Premium License or add-on is required.

j. **Microsoft PII Scans**
Scans OneDrive, email, and SharePoint files for personally identifiable information (PII). Discover, identify, and classify sensitive data. Please Note: Microsoft Business Premium License or add-on is required
i. Scans are performed on an agreed-upon schedule based on Client needs and/or compliance requirements.

k. **Mobile Device Management & Support**
Mobile Device Management (MDM) services protect your network by ensuring that devices are optimized and in a more secure state before allowing access. Please Note: Microsoft Business Premium license for users is required.
i. Secure Provisioning and Management
1. Comprehensive Device Enrollment: Facilitate the secure enrollment of mobile devices into your network, leveraging Microsoft Intune's robust capabilities to ensure a smooth and secure integration process.
2. Policy Implementation and Management: Through Intune, deploy and manage security policies across all mobile devices, ensuring that they adhere to your IT security standards. This includes configuring device settings, managing application permissions, and ensuring the security of your data.
ii. Data Protection and Privacy
These services focus on safeguarding your data while respecting individual privacy:
1. Remote Wipe Capabilities: In the event of a lost or stolen device, remotely wipe corporate data from the device, ensuring that sensitive information remains secure. This process is carefully designed to

remove only Client data, preserving the individual's personal information.

2. Conditional Access and Compliance Policies: Set conditional access policies through Intune that help protect corporate data on mobile devices. Devices that do not comply with Your security policies can be restricted from accessing corporate resources until compliance is achieved.

iii. Device and App Management: Manage both the devices and the applications they access, ensuring that only approved apps can access corporate data and that devices are configured with the necessary security settings.

iv. Customizable Security Settings: Tailor the security settings and policies applied to mobile devices to Your unique needs, ensuring they align with specific requirements.

v. User Training and Support: Provide user training and support to ensure that your staff are knowledgeable about mobile device security practices and understand how to use their devices safely within the organization's IT environment.

l. **Multi-Factor Authentication (MFA)**

Implementation and facilitation of a multi-factor authentication solution from our designated Third-Party Provider.

i. MFA Setup and Configuration: Set up MFA across all your critical applications and systems.

ii. Ongoing Management: Continuously monitor and manage MFA settings to adapt to any changes in your security needs.

iii. User Support: Provide support and assistance to users for MFA setup, troubleshooting, and best practices.

iv. Security Audits: Regularly audit to ensure compliance and effectiveness of MFA implementation.

m. **Onboarding & Offboarding Staff**

Detailed and documented procedures for onboarding and offboarding team members in a timely and efficient manner. To maximize efficiency and accuracy in the transition processes, tools include:

i. Custom Digital Forms for HR: Provide your HR department or the appropriate party with digital onboarding and offboarding forms. These forms are designed to gather all necessary information in a structured, secure, and easy-to-complete manner.

ii. Streamlined Communication: The digital forms serve as a single point of submission for initiating onboarding or offboarding requests, ensuring that all relevant details are captured accurately and communicated directly to our IT management team.

iii. Automated Process Triggers: Submission of these forms automatically triggers the respective onboarding or offboarding processes within our systems, allowing for timely and coordinated actions across our teams.

iv. Onboarding includes:

1. Efficient Account and Access Setup: Utilizing information provided through the digital forms, swiftly set up user accounts, email, and grant access to necessary systems and applications.
2. Device Provisioning and Configuration: Based on role-specific requirements captured in the digital form, prepare and configure laptops, desktops, and mobile devices to ensure they're ready for immediate productivity.
3. IT Orientation and Training: Provide orientation sessions covering IT policies, security protocols, and technology resources, ensuring new team members are well-prepared to work securely and efficiently.

v. Offboarding process ensures data integrity and security:

1. Prompt Access Revocation and Data Management: Information from the digital offboarding form guides revocation of system access and the secure management of data on organization-issued devices.
2. Hardware Return and Certification: Oversee the return and data wiping of devices, with processes initiated based on details provided through the digital form, ensuring compliance and security.

n. **Operating System Migrations**

Provides management, support, and optimization for cloud-based software applications.

i. Workstations

1. Assess the workstations to be upgraded, considering hardware specifications, existing software, and user requirements.
2. Create a detailed upgrade plan, outlining the specific tasks, timelines, and potential challenges.
3. Communicate the upcoming workstation upgrade to your POC well in advance so that communication can be provided to end-users. Provide clear instructions on what to expect, any necessary preparations, and who to contact for support.
4. Utilize the automation capabilities of our RMM tool to create deployment policies for the workstation upgrade.
5. Specify the target workstations, deployment schedule, and any additional configurations needed during the upgrade process.
6. Implement a phased or controlled rollout strategy to upgrade workstations in batches, starting with a small subset of users. This allows for close monitoring and quick response to any unforeseen issues.
7. After the upgrade, conduct a thorough post-upgrade validation to ensure that the new workstations are functioning as expected.

ii. Servers

Operating system upgrades are completed via a separate Professional Services engagement.

o. **Patch Management and Deployment for Servers**

Patch management for servers helps ensure the security, stability, and performance of your server infrastructure.

i. Develop and implement a standard server patching policy for your organization.
ii. Schedule patch scans and deployments for servers in accordance with an agreed upon schedule. Standard schedule is to deploy patches the Saturday following Microsoft's Patch Tuesday to ensure timely application of security updates.
iii. Configure automated patch scans specifically for servers. Servers run different software stacks and services; ensure the RMM tool can identify and manage updates for server-specific applications.
iv. Set up automated deployment rules for servers, considering maintenance windows and potential service disruptions. Ensure that updates are applied consistently across the server fleet.
v. Utilize a rollback mechanism for servers to quickly revert to a stable state in case a patch causes issues.
vi. Enable monitoring features to track the patch status of servers. Receive alerts for failed patch installations or any issues that may impact server performance or security. Regularly review patch management reports for servers to assess the overall security and compliance status.
vii. Extend patch management capabilities to cover certain third-party software on servers.
viii. Keep comprehensive documentation of server patch management processes, including schedules, policies, and any specific considerations for different server roles.

p. **Patch Management and Deployment for Workstations**

This service maintains the security and performance of your computer systems. Our Remote Monitoring and Management (RMM) is used to automate and streamline the process.

i. Define patching policies based on the specific needs and requirements of your organization. This includes determining the frequency of patch scans and installations.
ii. Microsoft typically releases security updates on the second Tuesday of each month, known as "Patch Tuesday." Configure our RMM tool to schedule patch scans and deployments shortly after this day to ensure that critical updates are applied promptly.
iii. Set up automated patch scans to identify missing patches on workstations. Our RMM tool scans all endpoints and generates reports on missing updates that guide our Centralized Services Engineer.
iv. Configure automated deployment rules to install approved patches during specified maintenance windows to minimize disruption to end-users while ensuring timely updates.
v. Enable monitoring features to track the patch status of workstations. Receive alerts for failed patch installations or any issues that may arise during the patching process.

vi. Regularly review patch management reports to assess the overall security posture of your workstation environment.

q. **Printer/Scanner/Copier Management & Support**

These services improve printing efficiency by managing your office printers and multifunction devices so that they are accessible to all employees.

i. Cloud Based Print Management

Implement a cloud-based print management solution to simplify and automate the process of managing printers and print jobs.

1. Deployment & Configuration: Complete the initial setup and configuration of Printix solution, ensuring all printers and user accounts are properly integrated.
2. Ongoing Management: Continuously monitor and manage the print environment, making updates and adjustments as needed to maintain optimal performance.
3. User Support: Comprehensive service desk support for any print-related issues, assisting users with troubleshooting and problem resolution.
4. Reporting & Analytics: Generate and review detailed print usage reports, helping to identify cost-saving opportunities and optimize printing policies.

ii. Network Support for Printers and Scanners

1. Network Configuration and Optimization: Ensure optimal configuration of printers and scanners on your network, enhancing device communication and performance.
2. Troubleshooting and Resolution: Troubleshoot any network-related issues affecting printers and scanners to ensure minimal downtime and maintained productivity.
3. Proactive Network Monitoring: Utilize advanced tools to proactively monitor the network connectivity of printers and scanners; identify and resolve potential issues before they impact operations.

iii. Copier Support

1. Network Integration Services: Facilitate the network integration of copiers, ensuring they are correctly configured for network printing and scanning functionalities.
2. Network Performance Monitoring: Monitor the network performance of copiers to ensure reliable operation and quickly address any network-related issues.
3. Supplier Coordination: Act as a liaison between you and your copier suppliers, coordinating support and maintenance for physical issues and ensuring that any needed physical repairs or maintenance are addressed promptly and effectively by the supplier.
4. Advisory Services: Advise on best practices for managing and negotiating support contracts with copier suppliers, helping ensure you receive optimal service and value.

r. **Remote Monitoring and Management**

RMM provides comprehensive oversight of your IT infrastructure. This service ensures continuous monitoring of your systems and immediate alerting in case of any issues, enabling proactive management and swift resolution of potential problems.

i. 24/7 Monitoring: Round-the-clock monitoring of your network, servers, workstations, and other critical systems. This continuous vigilance helps in early detection of issues before they escalate into major problems.

ii. Automated Alerts: In the event of an anomaly or issue, system-generated alerts are immediately sent to our team, ensuring prompt attention and action.

iii. Customizable Monitoring Parameters: Tailor monitoring to your specific needs, focusing on critical systems and components essential for your operations. This customization ensures that monitoring is relevant and effective.

iv. Preventive Maintenance: Perform regular system checks and updates to prevent issues from arising. This includes patch management, performance optimization, and security updates.

v. Remote Diagnostics and Issue Resolution: Upon receiving an alert we diagnose and resolve issues remotely when possible, leading to faster response times and minimized disruption.

vi. Detailed Reporting: Provide reports detailing the health and performance of your IT infrastructure. These reports include insights on detected issues, resolved problems, and recommendations for improvements.

1. Workstations (desktop, laptop)
2. Servers
3. Network infrastructure (switches, routers, firewalls)

s. **Remote Service Desk**

Remote Service Desk provides efficient, responsive, and high-quality IT support to your organization. This service leverages the advanced features of our Professional Services Automation (PSA) platform to manage and resolve IT issues swiftly and effectively, helping to ensure minimal downtime and maximum productivity for your organization.

i. Centralized Ticketing System: Provide efficient tracking, management, and resolution of IT issues. You may create tickets via email, phone, or a self-service portal, ensuring easy access for your employees.

ii. Automated Issue Routing: The system automatically categorizes and routes tickets to the appropriate IT personnel based on the nature of the issue and skill set required. This leads to quicker response times and more effective resolutions.

iii. Remote Troubleshooting and Support: Provide remote troubleshooting and support, resolving issues without the need for on-site visits. This remote capability ensures faster response and resolution times.

iv. Service Level Agreements (SLAs): Goal is to meet stated response targets 90% of the time or greater and resolution targets 85% or greater.

v. Comprehensive Reporting and Analytics: Provide detailed reports on service desk performance, including resolution times, ticket volumes, and user satisfaction. These insights help in continually improving the service and addressing any areas of concern.

t. **Security Awareness Training and Phishing Service**

Implementation and management of a solution that is designed to educate and empower your employees to be the first line of defense against cyber threats. Utilizing our designated third party, this service provides training and simulation exercises to enhance the cybersecurity awareness and behavior of your team.

i. Interactive Training Modules
ii. Simulated Phishing Attacks
iii. Tracking and Reporting

u. **Software Licensing (applies to software purchased through Data Networks)**

i. All software provided to you by or through Data Networks is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Data Networks' Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.
ii. When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

v. **Strategic IT Planning**

This service, provided by a Technology Success Manager, provides strategic technology leadership and guidance.

i. Develop and align the technology strategy with your overall operational goals and objectives. Provide insights into how technology can support and enhance your organization's long-term plans.
ii. Assist in the development of IT budgets and plans that align with your financial objectives. Ensure that technology investments are prioritized based on operational needs.
iii. Identify and assess technology-related risks and vulnerabilities. Develop strategies to mitigate risks, including cybersecurity threats and data breaches.
iv. Evaluate and manage relationships with technology vendors and service providers. Negotiate contracts and agreements to ensure cost-effectiveness and service quality.
v. Assess and recommend improvements to your technology infrastructure. Ensure that the IT environment is scalable, secure, and aligned with industry best practices.

vi. Establish IT governance frameworks to ensure compliance with regulations and industry standards. Oversee the implementation of security policies and procedures.
vii. Develop plans for business continuity and disaster recovery. Ensure that systems and data are protected and recoverable in the event of disruptions. Advise on digital transformation initiatives to leverage technology for innovation and efficiency. Identify opportunities for automation and process improvement.
viii. Work closely with your executive team to align technology initiatives with broader organizational strategies. Communicate the value of technology investments in terms of business outcomes.
ix. Oversee the performance and development of IT staff. Provide leadership and mentorship to the IT team as requested by Client.
x. Engage in strategic planning sessions to ensure that technology considerations are integrated into the overall organizational strategy. Anticipate future technology trends and their potential impact on the organization.
xi. Provide regular reports to executive leadership on the status and performance of IT initiatives. Conduct periodic reviews to ensure alignment between technology activities and organizational goals.

w. **Technology Alignment**

Technology Alignment is based on a developed and maintained library of technology standards. This service, provided by a Technology Alignment Engineer, includes:

i. Develop and maintain technical knowledge of your IT environment and benchmark your infrastructure against our library of technology standards.
ii. On a regular schedule, conduct assessments of your IT infrastructure against technology standards to determine deficiencies or vulnerabilities.
iii. Communicate the technical findings of assessments to your assigned Technology Success Manager.
iv. Schedule onsite meetings to provide regular updates and reports on MSP activity, such as service desk tickets trends. Address any concerns or issues and ensure a positive relationship through effective communication and responsiveness.

x. **Vendor and Procurement Management**

This service includes assistance with managing the entire lifecycle of your IT assets, including procurement, deployment, maintenance, replacement, and decommissioning. Procurement Management includes vendor management, purchasing, licensing management, supply chain management, and budget management. Our Technology Success Manager ensures that procurement management is aligned with strategic IT planning and lifecycle management.

Your Technology Success Manager will assist in the evaluation and relationship management of technology vendors and service providers. The goal is to ensure that the interplay between you and your vendors is smooth, efficient, and beneficial for both parties. Key aspects of vendor management include:

i. Vendor Selection and Onboarding: Assist in choosing the right vendors based on your needs, negotiating contracts, and managing the onboarding process to ensure that vendors understand your requirements and expectations.
ii. Contract Management: Handle critical aspects of vendor contracts, including negotiation, renewals, and termination. Secure favorable terms for you while helping to ensure that service levels and deliverables are clearly defined and met.
iii. Relationship Management: Serve as the primary point of contact between you and your IT vendors, facilitating communication, resolving conflicts, and fostering collaboration.
iv. Cost Optimization: Strive to achieve cost savings for you by leveraging relationships with key IT vendors, consolidating services where possible, and negotiating better rates or terms.
v. Strategic Alignment: Ensure that the services and products sourced from vendors align with your strategic goals. Your Technology Success Manager plays a key role in aligning vendor capabilities with your objectives and technology roadmap.

You are required to have valid maintenance contracts in place with the manufacturers or suppliers of the goods or services implemented in your IT environment. If an issue arises, Data Networks will work to identify the root cause of the issue and interface with the manufacturer, if needed, for resolution.

y. **Vulnerability Scanning and Management**
Implementation of Vulnerability Management provides comprehensive scanning, assessment, and management of vulnerabilities across your network by our designated third party. This service is essential for identifying and addressing security weaknesses before they can be exploited by cyber attackers.
i. Comprehensive Vulnerability Scanning: Perform a deep scan across your network. Scan covers all devices, applications, and systems, identifying vulnerabilities such as unpatched software, insecure configurations, and other security weaknesses.
ii. Regular and On-Demand Scans: Schedule and perform on-demand scans to ensure continuous vulnerability assessment. This flexibility allows for immediate scanning in response to new threats or changes in your network.
iii. Detailed Reporting and Analysis: Provide a detailed report after each scan outlining the identified vulnerabilities, their severity, and potential impact on your network. Reports also include actionable recommendations for remediation.
iv. Prioritization of Risks: Prioritize vulnerabilities based on their severity and the potential threat they pose to your organization. Prioritization helps focus remediation efforts on the most critical vulnerabilities first.
v. Remediation Guidance and Support: Provide expert guidance on addressing identified vulnerabilities. Assist in developing and implementing remediation strategies to mitigate risks effectively.

vi. Compliance Assurance: The service aids in compliance with various regulatory standards by helping to ensure your network is free from known vulnerabilities.

z. **Workstation Deployment (for devices purchased from Data Networks)**

i. Seamless Deployment for Machines Purchased from Data Networks. For PCs and devices purchased directly from Data Networks, we provide:

1. Complimentary Setup and Configuration: No-cost setup and configuration service for all machines purchased through us. This includes installation of standard software applications, network configuration, and user settings, ensuring that devices are ready for immediate use.
2. Custom Configuration Services: Custom configuration services to meet specific operational requirements or preferences. This service is designed to ensure that each PC is tailored to support the unique needs of your users and workflows.

ii. Fixed-Price Deployment for Machines Purchased Externally

Recognizing that you may source machines from external providers, Data Networks extends its PC deployment services to include:

1. Fixed-Price Setup and Configuration: For devices not purchased through Data Networks, we offer a fixed-price deployment service available via a separate Professional Services engagement. This includes the same high level of setup and configuration provided for our direct sales, ensuring that all machines, regardless of their source, are integrated seamlessly into your IT environment.
2. Transparent Pricing Structure: We believe in full transparency and will provide upfront pricing for the setup and configuration of externally sourced machines. This fixed-price approach ensures that you can budget accurately for deployment services without concerns about unexpected costs.

aa. **Workstation Management**

Managing your workstations using specific tools for Windows and Mac operating systems.

i. Windows Workstation Management Tool

1. Device Enrollment: Use our Remote Monitoring and Management tool to provide seamless device enrollment, enabling users to connect their Windows devices quickly and securely to organizational resources.
2. Configuration Profiles: Create configuration profiles to enforce settings on Windows devices, including Wi-Fi, VPN, and security configurations.
3. Application Deployment: Use our Remote Monitoring and Management tool to facilitate the deployment of applications to Windows devices. This includes the ability to install, update, or remove applications remotely.

4. Security Policies: Use our Remote Monitoring and Management tool to enforce security policies on Windows devices, such as BitLocker encryption settings, EDR configurations, and compliance policies.
5. Conditional Access: Implement Conditional Access policies to ensure that only compliant and secure devices can access organizational resources, enhancing overall security.

ii. Mac Workstation Management Tool

1. Device Enrollment: Use our Mobile Device Management tool to streamline the enrollment process for Mac devices, allowing users to easily connect their devices to the management platform. Utilizing your organization's Apple Business Manager, we create an automated workflow that auto enrolls a device upon purchase from Apple.
2. Policy Configuration: Create and enforce policies for macOS devices, covering configurations for security settings, network preferences, and system preferences.
3. Software Deployment: Our Mobile Device Management Solution supports software deployment on Mac devices, enabling us to install, update, and remove applications remotely.
4. Security and Compliance: Implement security controls and compliance policies to ensure that Mac devices adhere to organizational security standards.
5. Remote Management: Our Mobile Device Management tool provides remote management capabilities, allowing our team to troubleshoot issues, install updates, and perform maintenance tasks on Mac devices remotely.
6. Inventory and Asset Management: Our Mobile Device Management tool offers inventory and asset management features to track hardware and software details across Mac devices.
7. Patch Management: Our Mobile Device Management tool assists in managing macOS updates and patches, ensuring that devices are kept current with the latest security fixes.
8. Automated Workflows: Our Mobile Device Management tool allows for the creation of automated workflows to streamline repetitive tasks, increasing efficiency in device management.

3. Recurring Services – Managed Modules

Managed Modules are available as an add-on to base services at additional cost. Options you select are included in the Quote.

a. **Managed Business Continuity and Disaster Recovery (BCDR)**
Implementation and facilitation of a backup monitoring solution from our designated Third-Party Provider. Features include:

i. On-Premises Backups

1. Backup Management:

Manage the regular backup of critical data and systems on-premises. This includes configuring backup schedules, selecting appropriate backup methods (full, incremental, differential), and ensuring that backups are performed reliably.

2. Recovery Process:
    A. Data Restoration: In the event of data loss or system failure, initiate the restoration process using on-premises backup data. This involves retrieving the most recent and relevant backup and restoring data and applications to their previous state.
    B. System Recovery: For more severe cases like hardware failures, Data Networks may perform full system recoveries, which include reinstalling operating systems and applications, followed by data restoration.
    C. Testing and Validation: Regularly test backup systems to ensure data can be effectively restored. Includes validating the integrity of the recovered data and systems.
    D. Disaster Recovery Planning: Assist in developing on-premises disaster recovery plans that detail how recovery is executed in various scenarios, ensuring minimal downtime.

ii. Cloud Backups

1. Data Encryption and Security: This service Ensures that data is encrypted during transfer to and from the cloud and remains secure while stored in the cloud.
2. Recovery Process:
    A. Remote Data Retrieval: In case of a disaster, data is retrieved from the cloud using efficient processes to minimize downtime.
    B. Virtualized Recovery: Often, Data Networks utilize cloud-based virtual machines to quickly restore services, enabling rapid resumption of operational functions.
    C. Application-Specific Recovery: Some cloud services allow for application-specific backups (e.g. databases or email systems), and Data Networks manage the recovery of these applications directly from the cloud.
    D. Testing and Compliance: Regularly testing cloud-based recovery processes and ensuring that they comply with data governance and regulatory requirements.
3. Cloud Continuity Strategy: Developing strategies that leverage cloud computing for business continuity. This might involve setting up redundant cloud services or using cloud environments for emergency operations.
    A. Unlimited Data retention
    B. Spinning up environment to run from cloud.

b. **Managed Compliance**

This service helps your organization prepare for, earn, and maintain compliance with multiple global regulations that include CMMC, GDPR, HIPAA, NIST, CSF, and PCI, plus manage due care for your Cyber Liability Insurance.

An initial assessment is conducted for each standard selected and incurs a separate cost. One monthly fee then covers compliance management for all your selected standards regardless of the number.

i. Assessment: Assessment of your current environment and practices against identified compliance standards
    1. Analysis and regular reporting on gaps in compliance
    2. Recommendations for remedial actions

ii. Compliance Management: Following the initial assessment, reporting, and recommendations we monitor your compliance posture and guide you toward improved compliance with:
    1. Automated scans and reporting provided approximately every 30 days. This reporting identifies changes relative to the compliance items available via the automated scanning tools. It does not include items documented via Client questionnaires.
    2. Quarterly check-in and guidance meetings conducted approximately every 90 days. These meetings, conducted with a senior member of our service delivery team, will provide a review of your current compliance posture, a check on your compliance efforts, and recommended actions for the quarter ahead.
    3. A comprehensive reassessment is run approximately every 365 days. This reassessment is identical to the initial assessment and provides the same reporting and guidance.

Please Note: Managed Compliance requires your ongoing cooperation and participation. To the extent that you provide incomplete, inaccurate, or outdated information, results may be incorrect or incomplete and should not be relied upon.

c. **Managed Firewall (firewall appliance provided by Data Networks)**

An effective firewall prevents unauthorized users from accessing internal network(s) from outside the network(s), provides secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; and provides website content filtering functionality.

i. Install and configure Data Networks-supplied firewall appliance using best practices.

ii. Monitor, update (software/firmware), and support Data Network-supplied firewall appliance.

d. **Managed M365**

Specify, provision, manage, and support your Microsoft 365 environment to help ensure your organization receives a seamless Microsoft 365 experience. This service includes:

i. Administer your Microsoft 365 licenses
ii. Recommend the right license plans for best functionality and value
iii. Consolidate your monthly billing
iv. Remove the burden and stress of managing your M365 environment

e. **Managed SaaS Protection**

This service protects your data stored by cloud-hosted applications via an all-in-one backup, search, restore, and export solution. Managed SaaS Protection includes:

i. Cloud to cloud backup and recovery of data that resides in Microsoft 365 and/or Google Workspace applications
    1. Microsoft 365
        A. Exchange
        B. OneDrive
        C. SharePoint
        D. Teams
        E. Tasks
    2. Google Workspace
        A. Gmail
        B. Google Drive
        C. Calendar
        D. Contacts
        E. Shared Drive
ii. Protection against common types of data loss (malware, user error)
iii. Quick recovery from cloud data loss with non-destructive and cross-user restore capabilities
iv. Secure cloud-to-cloud backup (performed 3x daily) with point-in-time rollback to mitigate ransomware attacks
v. Effective monitoring and management including role-based administration and audit logs

Please Note: Successful implementation of this service is predicated on the following:

- No changes will be made to your backup environment without notifying Data Networks
- No significant changes will be made to your M365 tenant or Google Workspace tenant without notifying Data Networks
- Data Networks' technical staff will be granted all required access in a timely fashion

4. Professional Services

Available at additional cost, Data Networks Professional Services provide access to qualified technical resources to perform work not covered under our base Managed IT Services or Managed Modules (e.g. modernization or upgrade recommendations from your Technology

Success Manager as part of the Strategic IT Planning process). Professional Services may be purchased as part of a project or pre-paid through an IT Services Retainer.

a. Professional Services Projects
   Professional Services Projects are offered on a fixed-price basis.
   i. Project scope, services, timeline, pricing, and terms will be provided to you in a formal Statement of Work ("SOW").
   ii. Your signature on the SOW and/or a valid PO is required for project initiation.

b. IT Services Retainer
   Our IT Services Retainer Program lets you pre-pay for professional services to supplement your Managed IT Services contract.
   i. You purchase one or more blocks of technical support hours ("IT Retainer") and we provide an appropriate professional services resource(s) on an "as needed" basis ("Services").
   ii. The specific scope, timing, term, and pricing of the Services (collectively, "Specifications") will be determined between you and us at the time that you request an IT Retainer to be put in place.
   iii. You will receive a quote that specifies the retainer amount and hourly rates of various engineering levels.
   iv. Remote services/support may be consumed in 30-minute increments. Onsite services/support must be consumed as a minimum 4-hour block and 30-minute increments thereafter (same day).
   v. All retainer contracts run from January 1 to December 31 (unless otherwise agreed to and specified on the quote) and are billed upfront via credit card or ACH. Unused funds expire at contract end. You will receive a 90-day notification of contract expiration to assist with planning and renewal.
   vi. You will receive a statement on the first Friday of each month detailing the retainer amount used by engineer level, the balance remaining, and the expiration date on the remaining balance.
   vii. Unless we agree otherwise in writing, services will be provided only during our normal business hours, which are currently 7am – 5pm Eastern Standard Time. Services provided outside of our normal business hours are subject to increased fees and technician availability and require mutual consent to implement.
   viii. The priority given to implementing the Services will be determined at our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an email from Data Networks. If no specific milestone or deadline is agreed upon, then the Services will be scheduled on a "best effort" basis to meet your needs, the specific requirements of the job(s), and technician availability.

Please Note: All Managed Services Clients receive a 20% discount on Professional Services. To learn more about our Professional Services capabilities, experience, and certifications visit our website at www.datanetworks.com.

5. Covered Environment

Managed Services will be applied to the number of users and/or related devices indicated in the Quote ("Covered Users/Devices"). The list of Covered Users/Devices may be modified by mutual consent (email is sufficient for this purpose); however, we reserve the right to modify the list of Covered Users/Devices at any time if we discover users/devices that were not previously included in the list of Covered Users/Devices and which are receiving Services, or as necessary to accommodate changes to the quantity of Covered Users/Devices.

Unless otherwise stated in the Quote, Covered Users/Devices will only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Data Networks may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to two (2) Business Devices used by the number of users indicated in the Quote. A "Business Device" is a device that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii) has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device.

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis only and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation, not an obligation, to you.

If we are unable to remediate an issue with non-Supported Software, then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software and if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

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. Data Networks 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 Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

6. Minimum Requirements/Exclusions

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be always provided/maintained by Client:

- All hardware must be of commercial grade with an active manufacturer's warranty.
- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine and licensed with active vendor or OEM support.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported enterprise-class backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- 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.
- Client 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.
- Client must provide us with exclusive administrative privileges to the Environment.
- Client 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.
- Client must have an Active Directory domain environment.
- Client must maintain a third-party support agreement for LOB applications.
- Client must have broadband internet access of at least 5Mb/s download and 1Mb/s upload speeds.
- Client must have properly sized and operational Uninterruptable Power Supply (UPS).

The following minimum requirements apply to Client workstations:

- Processor (CPU):
    - Intel Core i5 or equivalent AMD processor

    - No older than 5 generations from the latest available models
- Memory (RAM):
    - Minimum: 8GB RAM
    - Recommended: 16GB RAM
- Storage:
    - Minimum 256GB Solid State Drive (SSD) for faster performance and reliability
- Operating System:
    - Minimum oldest iteration supported by the manufacturer
- Network Connectivity:
    - Gigabit Ethernet for wired connections
    - Support for Wi-Fi 5 (802.11ac) or Wi-Fi 6 (802.11ax) for wireless connectivity
- Ports:
    - Sufficient USB ports, including USB-A and USB-C, for connecting peripherals
    - HDMI or DisplayPort for external displays
- Warranty and Support:
    - Devices are covered under a valid manufacturer warranty and appropriate support plans
    - Accidental damage warranty for laptop
    - For any device not under warranty, support will be provided on a "best effort" basis

Exclusions

Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Data Networks. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Data Networks 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 managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- 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.
- Replacement parts.
- Break fix for out-of-warranty devices.
- One time project work.
- LOB application support without a current vendor support contract.
- Home office equipment.

- Upgrades to LOB/specialty applications.
- Building security system support.
- Changing data backup media (tapes or cartridges).
- Specialty equipment (e.g., medical devices, point of sale, specialty printers, etc.).
- Video conferencing/projector equipment.
- Linux support.
- Copier support.
- Cabling support.
- Non-corporate system support.
- Environmental disposal fees.
- Consumer software and hardware support.

Best Effort Support

For service requests or issues may fall outside the defined scope of managed services, covered systems, or vendor-supported configurations. In these cases, Data Networks will provide "Best Effort" support. This means our technical team will make every reasonable attempt to assist the client using available resources and professional expertise, but without a guaranteed resolution time, service restoration, or successful outcome.

Best Effort support is typically provided for up to the first hour at no additional charge as a courtesy to evaluate and attempt resolution. If the issue requires further time, specialized resources, or third-party engagement beyond that initial hour, additional labor or vendor costs may be billed separately with the client's prior approval. This approach ensures transparency while allowing clients to make informed decisions about continuing work that falls outside the standard service scope.

7. 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-F, 7AM – 5PM Eastern Time, excluding legal holidays and Data Networks-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by Data Networks in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Data Networks will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Priority Level	Description	Examples	Response	Resolution
Priority 1	Critical issues that severely impact business operations. These issues require an immediate response to minimize downtime and prevent significant business disruptions.	▪ Complete network outage affecting multiple users. ▪ Critical server failure. ▪ Security breach or data loss incident.	30 mins	4 hours
Priority 2	High-priority issues that need attention promptly but may not be as severe as Priority 1 issues. Resolving Priority 2 issues is crucial to maintain normal business.	▪ Service disruptions for a specific department. ▪ Critical software application failure. ▪ High-priority hardware malfunctions.	1 hour	8 hours
Priority 3	Issues that are important but do not require immediate attention. These issues may impact productivity, but workarounds or alternative solutions may be available.	▪ Individual user system issues. ▪ Software glitches impacting a small group of users. ▪ Non-critical hardware malfunctions.	4 hours	24 hours
Priority 4	Non-urgent issues that have minimal impact on business operations. These issues may involve routine requests, inquiries, or non-critical tasks.	▪ General information requests. ▪ Password resets for users with no immediate deadlines. ▪ Non-urgent software feature requests.	8 hours	48 hours

*All time frames are calculated as of the time that we are notified of the applicable issue/problem by Client through our designated support portal, help desk, or by telephone at the telephone number listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Support During Off-Hours/Non-Business Hours

Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Data Networks agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on

a time and materials basis (which is not covered under any Service plan) and will be billed to Client at 1.5x our then-current hourly rates.

All hourly services are billed in 30-minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

Data Networks-Observed Holidays

Data Networks observes the following holidays:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Eve

8. Fees

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

Reconciliation. Fees for certain Third-Party Services that we facilitate or resell to you may begin to accrue prior to the "go-live" date of other applicable Services. (For example, Microsoft Azure related fees begin to accrue on the first date on which we start creating and/or configuring certain hosted portions of the Environment; however, the Services that rely on Microsoft Azure may not be available to you until a future date). You understand and agree that you will be responsible for the payment of all fees for Third Party Services that are required to begin prior to the "go-live" date of Services, and we reserve the right to reconcile amounts owed for those fees by including those fees on your monthly invoices.

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 authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Travel Time. If onsite services are provided, we will travel up to 45 minutes from our office to your location at no charge. Time spent traveling beyond 45 minutes (e.g., locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) 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.

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 a 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.

Access Licensing. One or more of the Services may require us to purchase certain "per seat" or "per device" licenses (often called "Access Licenses") from one or more Third Party Providers. (Microsoft "New Commerce Experience" licenses as well as Cisco Meraki "per device" licenses are examples of Access Licenses.) Access Licenses cannot be canceled once they are purchased and often cannot be transferred to any other Client. For that reason, you understand and agree that regardless of the reason for termination of the Services, fees for Access Licenses are non-mitigatable and you are required to pay for all applicable Access Licenses in full for the entire term of those licenses. Provided that you have paid for the Access Licenses in full, you will be permitted to use those licenses until they expire.

9. 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 Data Networks' satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this Service Guide (the "Service Term").

Per Seat/Per Device Licensing. Regardless of the reason for the termination of the Services, you will be required to pay for all per seat or per device licenses that we acquire on your behalf. Please see "Access Licensing" in the Fees section above for more details.

Removal of Software Agents; Return of Firewall & Backup Appliances. 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 managed environment or any of the devices on which we installed software agents. 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 software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, you must remove, package and ship, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise provided to you by Data Networks "as a service." If you fail to timely return all such 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.

10. Offboarding

Subject to the requirements in the MSA, Data Networks will off-board Client from Data Networks' services by performing one or more of the following:

a. **Notification and Offboarding Planning**
   i. Acknowledge receipt of the Client's termination request.
   ii. Schedule an offboarding meeting to discuss the process, timeline, and any specific requirements.

b. **Secure Data Handling and Transfer**
   i. Coordinate the secure transfer of client data, ensuring encryption and compliance with data protection regulations.
   ii. Assist with data migration to the new service provider, if applicable.

c. **Decommissioning of Services**
   i. Remove RMM, EDR, and MDR agents from all client devices.
   ii. Decommission any deployed network security solutions, such as firewalls.

d. **Asset and Documentation Handover**
   i. Provide the Client with a final inventory of all devices, software, and assets.
   ii. Hand over all documentation related to the Client's IT infrastructure, configurations, and procedures.

e. **Final Account Settlement**
   i. Prepare and send the final invoice, including any prorated charges or refunds.
   ii. Ensure all financial obligations are settled.

f. **Feedback and Exit Interview**
   i. Conduct an exit interview to gather feedback and discuss the Client's experience.
   ii. Document insights and feedback for internal review and improvement.

g. **Data Deletion and Privacy Compliance**
   i. Securely delete all client data from your systems in compliance with data protection laws and regulations.
   ii. Confirm the completion of data deletion to the Client.

11. Additional Policies

The following additional policies ("Policies") apply to Services that we provide or facilitate under a Quote. By accepting a Service for which one or more of the Policies apply, you agree to the applicable Policy.

1. **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.

2. **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 Data Networks, and Client shall not modify these levels without our prior written consent.

3. **Configuration of Third-Party Services**

Certain third-party services provided to you under a Quote 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 authorization could disrupt the Services and/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.

4. **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.

5. **Advanced Endpoint Protection & Response (EDR)**

Our EDR solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists 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 Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that Data Networks 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.

6. **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 or systems impacted by the incident will be recoverable or remediated. 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 Client'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 managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

7. **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.

8. **Fair Usage Policy**

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable 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 engineers' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our engineers 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 Clients.

9. **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—including ours. 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 Data Networks 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. Data Networks reserves the right, but not the obligation, to suspend Client's access to the Hosted Email and/or all transactions occurring under Client's Hosted Email account(s) if Data Networks believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

10. **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 Client's data. Neither Data Networks 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. Data Networks cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Data Networks shall be held harmless if such data corruption or loss occurs. Client is strongly advised to keep a local backup of all stored data to mitigate against the unintentional loss of data.

11. **Procurement**

Equipment and software procured by Data Networks on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, Data Networks 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 Client's responsibility if a return of the Procured Equipment is requested. Data Networks is not a warranty service or repair center. Data Networks will facilitate the return or warranty repair of Procured Equipment; however, Client 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 Data Networks will be held harmless, and (ii) Data Networks 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.

12. **Business Review/IT Strategic Planning Meetings**
We strongly suggest that you participate in business review/strategic planning meetings as may be requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

13. **Strategic IT Planning Services**
The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer (if applicable) will be for your informational and/or educational purposes only. Data Networks will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Data Networks on Client's corporate records or accounts.

14. **Sample Policies, Procedures.**
From time to time, we may provide you with sample (i.e., template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your Clients') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your Clients') business operations.

15. **Penetration Testing; Vulnerability Scanning**
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 and/or vulnerability scanning processes, 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 or vulnerability scanning 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 or vulnerability scanning 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.

16. **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 are 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.

17. **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, or (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose). 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.

18. **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.

19. **VOIP – Dialing 911 (Emergency) Services**

The following terms and conditions apply to your use of any VoIP service that we facilitate for you or that is provided to you by a third-party provider of such service. Please note, by using VoIP services you agree to the provisions of the waiver at the end of this section. If you do not understand or do not agree with any of the terms below, you must not subscribe to, use, or rely upon any VoIP service and, instead, you must contact us immediately.

There is an important difference in how 9-1-1 (i.e., emergency) services can be dialed using a VoIP service as compared to a traditional telephone line. Calling emergency services using a VoIP service is referred to as "E911."

Registration. You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service. This will not be done for you, and you must take this step on your own initiative. To do this, you must log into your VoIP control panel and provide a valid physical address. If you do not take this step, then E911 services may not work correctly, or at all, using the VoIP service. Emergency service dispatchers will only send emergency personnel to a properly registered E911 service address.

Location. The address you provide in the control panel is the location to which emergency services (such as the fire department, the police department, etc.) will respond. For this reason, it is important that you correctly enter the location at which you are using the VoIP services. PO boxes are not proper addresses for registration and must not be used as your registered address. Please note, even if your account is properly registered with a correct physical address, (i) there may be a problem automatically transmitting a caller's physical location to the emergency responders, even if the caller can reach the 911 call center, and (ii) a VoIP 911 call may go to an unstaffed call center administrative line or be routed to a call center in the wrong location. These issues are inherent to all VoIP systems and services. We will not be responsible for, and you agree to hold us harmless from, any issues, problems, incidents, damages (both bodily- and property-related), costs, expenses, and fees arising from or related to your failure to register timely and correctly your physical location information into the control panel.

Address Change(s). If you change the address used for E911 calling, the E911 services may not be available and/or may operate differently than expected. Moreover, if you do not properly and promptly register a change of address, then emergency services may be directed to the location where your services are registered and not where the emergency may be occurring. For that reason, you must register a change of address with us through the VoIP control panel no less than three (3) business days prior to your anticipated move/address change. Address changes that are provided to us with less than three (3) business days' notice may cause incorrect/outdated information to be conveyed to emergency service personnel. If you are unable to provide us with at least three (3) business days' notice of an address change, then you should not rely on the E911 service to provide correct physical location information to emergency service personnel. Under those circumstances, you must provide your correct physical location to emergency service dispatchers if you call them using the VoIP services.

If you do not register the VoIP service at your location and you dial 9-1-1, that call will be categorized as a "rogue 911 call." If you are responsible for dialing a rogue 911 call, you will be charged a non-refundable and non-disputable fee of $250/call.

Power Loss. If you lose power or there is a disruption to power at the location where the VoIP services are used, then the E911 calling service will not function until power is restored. You should also be aware that after a power failure or disruption, you may need to reset or reconfigure the device prior to utilizing the service, including E911 dialing.

Internet Disruption. If your internet connection or broadband service is lost, suspended, terminated or disrupted, E911 calling will not function until the internet connection and/or broadband service is restored.

Account Suspension. If your account is suspended or terminated, then all E911 dialing services will not function.

Network Congestion. There may be a greater possibility of network congestion and/or reduced speed in the routing of E911 calls as compared to 911 dialing over traditional public telephone networks.

WAIVER. You hereby agree to release, indemnify, defend, and hold us and our officers, directors, representatives, agents, and any third party service provider that furnishes VoIP-related services to you, harmless from any and all claims, damages, losses, suits or actions, fines, penalties, costs and expenses (including, but not limited to, attorneys' fees), whether suffered, made, instituted or asserted by you or by any other party or person (collectively, "Claims") arising from or related to the VoIP services, including but not limited to any failure or outage of the VoIP services, incorrect routing or use of, or any inability to use, E911 dialing features. The foregoing waiver and release shall not apply to Claims arising from our gross negligence, recklessness, or willful misconduct.

20. **Acceptable Use Policy**

The following policy applies to all hosted services provided to you, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, and hosted infrastructure services ("Hosted Services").

Data Networks does not routinely monitor the activity of hosted accounts except to measure service utilization and/or service uptime, security-related purposes and billing-related purposes, and as necessary for us to provide or facilitate our managed services to you; however, we reserve the right to monitor Hosted Services at any time to ensure your compliance with the terms of this Acceptable Use Policy (this "AUP") and our master services agreement, and to help monitor and ensure the safety, integrity, reliability, or security of the Hosted Services.

Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Hosted Services. Instead, we prefer to advise our Clients of inappropriate behavior and any necessary corrective action. If, however, Hosted Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Hosted Services without prior notice.

Violations of this AUP

The following constitute violations of this AUP:

Harmful or illegal uses. Use of a Hosted Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.

Fraudulent activity. Use of a Hosted Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.

Forgery or impersonation. Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.

SPAM. Data Networks has a zero tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.

Internet Relay Chat (IRC). The use of IRC on a hosted server is prohibited.

Open or "anonymous" proxy. Use of open or anonymous proxy servers is prohibited.

Cryptomining. Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.

Hosting spammers. The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our Clients to be listed in any of the various SPAM databases, is prohibited. Clients violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the Client agrees to remove all traces of the offending material immediately upon reconnection and agree to allow Data Networks to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.

Email/message forging. Forging any email message header, in part or whole, is prohibited.

Unauthorized access. Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, Data Networks' security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.

IP infringement. Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.

Collection of personal data. Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.

Network disruptions and sundry activity. Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.

Distribution of malware. Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.

Excessive use or abuse of shared resources. The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one Client may have a negative impact on all other Clients. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other Clients or the performances of our systems or networks.

Allowing the misuse of your account. You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

To maintain the security and integrity of the hosted environment, we reserve the right, but not the obligation, to filter content, Data Networks requests, or website access for any web requests made from within the hosted environment.

Revisions to this AUP: We reserve the right to revise or modify this AUP at any time. Changes to this AUP shall not be grounds for early contract termination or non-payment.