Effective January 27, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

PRE-PACKAGED SERVICE PLANS

A summary of a description of the services included in each plan are included below. The scope of each feature is further defined in the Managed Workstation, Managed Security Service, Data Backup and Disaster Recovery Service, Cloud and Hosting Services, Cyber Training Services, and other applicable sections of this Schedule of Services, and as limited by the Order and any referenced Third-Party Service Provider terms.

Shared Device Plan -- The Shared Device plan is an add-on service that allows Provider to install the tools to monitor and protect additional systems beyond the machines that your team uses day-to-day and is meant to be paired with a user support plan. This plan extends the same monitoring, endpoint protection, and patch management tools described under Managed Workstation and Managed Security Service to shared or non-primary devices only, and does not include separate Help Desk support, hardware replacement, or major hardware/software upgrades unless expressly included in the Order.

Email Support Plan -- Email only support. Client may submit support requests to the Help Desk via email only, during the hours and under the limitations described in the Help Desk Services portion of the Managed Workstation section, and this plan does not include phone support, on-site Support, project work, or any Services not otherwise specified in the Order.

Startup Plan -- Basic support for small / solopreneur businesses. This plan provides core remote Help Desk, monitoring, security, and backup features for up to the number of Users listed below, as more fully described in the Managed Workstation, Managed Security Service, and Data Backup and Disaster Recovery Service sections, and excludes on-site Support, hardware replacement, and major upgrades or projects unless expressly added in the Order.

- **Unlimited help desk support**
  End users may submit an unlimited number of support requests to the Help Desk via the supported channels set out under Help Desk Services, subject to the scope and limitations described in that section and the Order, and does not include project work or Services outside normal support (such as major deployments or migrations).
- **Up to 5 Users**
  Additional Users may be added by upgrading or at an additional fee.
- **Proactive Monitoring**
  Provider will use remote monitoring tools, as described under Desktop Monitoring and Management and Managed Security Service, to watch supported Devices and systems for alerts and performance issues and to initiate remote remediation where feasible, but it does not guarantee prevention of all incidents or include physical inspections, hardware replacement, or unsupported systems.
- **Basic Endpoint Protection**
  Provider will deploy standard antivirus and anti-malware software and management, such as those described under Core Security Services, Intelligent Antivirus and Anti-malware, deployed to covered Devices using third-party tools identified in the Order,

© Scott & Scott, LLP

and does not include advanced or premium security add-ons unless specifically noted in a higher-tier plan or the Order.

- **Daily Backup of Microsoft 365**
  Supported Microsoft 365 data (such as email, OneDrive, SharePoint or other workloads specified in the Order) will be backed up using Third-Party Service Providers as described in the Data Backup and Disaster Recovery Service section below, subject to stated retention and restore limitations, and is not itself a full disaster recovery solution for Client's entire environment.
- **SSL Certificate Monitoring**
  Provider will use monitoring tools to track the status and expiration of SSL certificates for in-scope domains or devices identified in the Order and will notify Client of upcoming expirations or detected issues, with any renewals, reconfigurations, or certificate purchases to be handled as otherwise agreed in the Order.
- **Device Management**
  Supported desktops, laptops, and other endpoints listed in the Order will be remotely configured, monitored, and maintained as described in the Desktop Monitoring and Management and Core Security Services sections, and does not include physical repair, replacement, or installation of new hardware unless separately ordered.
- **Patch Management**
  Provider will deploy and manage operating system and supported application updates, including monthly Microsoft patch management as described in Core Security Services, for covered Devices where vendor patches are available, but does not guarantee compatibility with all third-party applications or cover remediation of issues caused by vendor-released patches beyond commercially reasonable efforts.
- **24/7 Security Operations Center**
  Security events from covered Devices and systems will be monitored around the clock by the SOC, with threat detection and response activities performed as described in the Security Operations Center and Security Incident Event Management (SIEM) sections, subject to the technical and scope limitations of the deployed tools and Third-Party Service Providers.
- **Monthly Executive Summary Report**
  Provider will deliver a high-level written or electronic summary of key service activity and status (such as tickets, alerts, backup status, and notable security events) for the prior period, based on information available from the systems and Services described in this Schedule, and such reporting is informational only and does not constitute a warranty of system performance or security.

Essentials Plan -- For small businesses needing responsive IT support and basic security. This plan builds on Startup by adding support for more Users and basic network and vendor management, with Unlimited Help Desk Support, monitoring, endpoint protection, Microsoft 365 backup, and related services delivered as described in the Managed Workstation, Managed Security Service, Data Backup and Disaster Recovery Service, and Vendor Management sections, and excluding on-site Support, hardware replacement, and major upgrades except as specified in the Order.

- **Unlimited Help Desk Support**
  End users under this plan may open an unlimited number of support tickets with the Help Desk via the channels described under Help Desk Services, within the scope defined in that section and the Order, and does not include project work, after-hours work beyond what is specified, or activities outside standard support (such as large-scale deployments).
- **Up to 20 Users**

© Scott & Scott, LLP

Services included in the Essentials Plan apply only to the number of named or licensed Users not exceeding this limit, as identified in the Order, and additional Users require an upgraded plan or separate Order.

- **Support for Microsoft 365**
  Provider's Help Desk will assist covered Users with configuration and troubleshooting of Microsoft 365 services licensed through Provider or listed in the Order, consistent with Help Desk Services and Third-Party Cloud & SaaS Vendors provisions, but does not include custom application development, data migration projects, or services outside normal end-user support unless otherwise agreed.
- **Proactive Monitoring**
  Provider will deploy remote monitoring tools, as further described under the Desktop Monitoring and Management and Managed Security Service sections below, to continuously monitor supported endpoints and in-scope network devices for alerts and performance issues and to initiate remote remediation where appropriate, without guaranteeing prevention of all outages or security incidents.
- **Basic Endpoint Protection**
  Provider will deploy standard antivirus and anti-malware services and related management as outlined in Core Security Services, Intelligent Antivirus and Anti-malware for Devices covered by the Order, and does not include advanced security features that are reserved for higher-tier plans or separate security offerings.
- **Daily Backup of Microsoft 365**
  Supported Microsoft 365 data will be backed up on a daily schedule using Third-Party Service Providers, in line with the Data Backup and Disaster Recovery Service description (including retention and restore parameters) and any specific terms set forth in the Order, and is not a replacement for broader disaster recovery services.
- **SSL Certificate Monitoring**
  Provider will track and alert on expiration or status issues for SSL certificates covering in-scope domains and services as identified in the Order using monitoring tools, with actual certificate procurement, renewal, or installation handled as separately agreed.
- **Quarterly Business Review (QBR)**
  Provider will meet (virtually or in person) with Client's designated representatives up to once per calendar quarter to review service performance, ticket trends, backup and security status, and technology roadmap recommendations, based on information from the Services described in this Schedule, with any resulting projects or changes to be documented and priced separately in an Order.
- **Device Management**
  Provider will configure, monitor, and maintain covered endpoints (such as desktops and laptops) as outlined in Desktop Monitoring and Management and Core Security Services, including standard configurations and policy enforcement, but not including physical repair or replacement of devices or unsupported operating systems or applications.
- **Network Management**
  Provider will configure and manage in-scope firewalls, routers, switches, and related network components as described under Network Management and Firewall and VPN Remote Access in the Managed Security Service section, including segmentation and secure access consistent with the Order, but excluding cabling, physical construction, or unsupported third-party network equipment.
- **Patch Management**
  Provider will deploy and manage operating system and supported application patches for covered Devices, including monthly Microsoft patching as part of Core Security Services, using remote tools identified in the Order, but cannot guarantee that all third-party applications will be patched or that vendor patches will be error-free.

© Scott & Scott, LLP

- **Vendor Management**
  Provider will assist Client, as further described in the Vendor Management section, with coordination and communication with third-party IT and cloud vendors listed in the Order (such as internet, telecommunications, and SaaS providers), including escalation and issue tracking, but Provider is not responsible for the underlying vendors' performance or service-level failures.
- **24/7 Security Operations Center**
  Qualifying security telemetry from covered Devices and systems will be monitored and analyzed at all times by the SOC, with threat detection, investigation, and response activities performed in accordance with the Security Operations Center and SIEM descriptions, and subject to the scope of the deployed security tools and the Order.

Business Plan -- For growing companies needing stronger security and compliance. A comprehensive and all inclusive user plan for help desk support across your technology stack including PC/laptop hardware, software, network and wireless, security, and mobile. This plan includes all Essentials Plan services plus enhanced security, identity, and compliance features described in the Managed Security Service, Cyber Training Services, and related sections, with coverage and licensing for each feature determined by the Order and excluding hardware replacement and major projects unless specifically included.

- **Everything in Essentials Plan**
- **Up to 200 Users**
- **Directory integration**
  Provider will configure supported identity and directory services (such as Microsoft Entra ID / Active Directory or other directory platforms identified in the Order) so that Users and Devices covered by this plan can leverage centralized authentication and access control, in coordination with the Multi-Factor Authentication and Single Sign-On services described in the Managed Security Service section.
- **Single Sign-On (SSO)**
  For compatible cloud and on-premises applications identified in the Order, Provider will configure centralized authentication so Users can access multiple applications with a single set of credentials, as further described in the Multi-Factor Authentication Services / Password Credential Management Services section, subject to the capabilities and licensing of the applicable third-party platforms.
- **Multi-Factor Authentication (MFA)**
  Provider will enable and help administer multi-factor authentication for supported systems and applications listed in the Order, as further described in Multi-Factor Authentication Services / Password Credential Management Services, using third-party authentication tools, and does not guarantee compatibility with all legacy or third-party applications.
- **Enhanced Security**
  In addition to Basic Endpoint Protection, Provider will enable additional advanced security controls and monitoring features (such as web filtering, data loss prevention, and enhanced identity protections) available under the Managed Security Service and Security Operations Center sections for in-scope Users and Devices, as specified in the Order and subject to Third-Party Service Provider capabilities.
- **Password Manager**
  Provider will provision and help administer a supported password management solution for covered Users, as identified in the Order and in connection with the Password Credential Management Services description, but does not include custom development, integration with unsupported systems, or recovery of passwords outside the capabilities of the third-party tool.

© Scott & Scott, LLP

- **Semi-Annual Security Audit**
  Provider will, up to twice per year, perform a structured review of Client's in-scope systems and security configurations based on information from the Managed Security Service and, where applicable, Security Risk Assessment tools, and will provide a summary of findings and recommendations, with any remediation work or major configuration changes to be scoped and priced separately in an Order.
- **Web Content Filtering**
  Provider will implement and manage policies, using DNS Filtering and related tools described in the Managed Security Service and Ad Hoc Services sections, to restrict access from covered Devices to categories of websites deemed inappropriate or risky, within the technical and categorization limits of the third-party filtering service.
- **Data Loss Prevention**
  Provider will configure and manage DLP policies, as further described under Data Loss Prevention in the Ad Hoc Services section and any Microsoft 365 DLP capabilities referenced in this Schedule, to monitor and help prevent unauthorized transmission of sensitive data from covered systems, subject to the capabilities of the underlying platforms and to the specific locations and data types identified in the Order.
- **Quarterly vCIO Strategic Consultation**
  Up to once per calendar quarter, Client may consult with a designated virtual CIO regarding technology strategy, budgeting, and alignment of the services described in this Schedule with Client's business objectives, with any agreed projects, migrations, or significant changes to be documented and priced separately in an Order.
- **Email Protection**
  Provider will implement and manage email security measures such as spam and phishing filtering, malware scanning, and related controls for covered email services, using Spam Prevention, Anti-malware, and other security tools described in the Managed Security Service section and any Microsoft 365 security features referenced in this Schedule, subject to third-party platform capabilities.
- **Security Awareness Training (SAT)**
  Covered Users will be enrolled in the managed cybersecurity awareness training and phishing simulation program described under Cyber Training Services, with education, testing, and reporting features as outlined there and as limited by the licenses and scope specified in the Order.

Enterprise Plan -- For organizations with strict security compliance and insurance requirements. This plan includes all Business Plan services plus additional advanced identity, compliance, and Microsoft 365 security features (such as advanced eDiscovery, sensitivity labeling, and privileged identity controls) as described in the Managed Security Service, Data Backup and Disaster Recovery Service, and Cloud and Hosting Services sections, with coverage and licensing determined by the Order and excluding hardware replacement, physical infrastructure, and large-scale projects unless expressly included.

- **Everything in Business Plan**
- **Unlimited Users**
  There is no fixed numeric cap on the number of Users who may be assigned to the Enterprise Plan under the Order, provided that all such Users are properly licensed and billed as specified in the Order, and all other scope and service limitations in this Schedule continue to apply.
- **Quarterly Virtual vCISO Check-In**
  Up to once per calendar quarter, Client may consult remotely with a designated virtual Chief Information Security Officer to review security posture, compliance considerations, and alignment of Managed Security Service features with applicable

© Scott & Scott, LLP

requirements, with any formal compliance assessments, certifications, or remediation projects to be separately scoped and documented in an Order.

- **Litigation Hold**
  Provider will, upon Client's written direction and subject to the capabilities of the applicable platforms (such as Microsoft 365), configure and help administer legal hold or retention features to preserve specified data for legal or regulatory purposes, consistent with the relevant Third-Party Service Provider tools and limitations, with legal strategy and compliance determinations remaining Client's responsibility.
- **Passwordless Authentication**
  Provider will assist with enabling supported passwordless sign-in methods (such as FIDO keys or platform authenticators) for compatible systems and applications identified in the Order, in coordination with directory integration and MFA services described in the Managed Security Service section, subject to the features and licensing of the applicable identity platforms.
- **"Always On" VPN**
  Provider will configure and help maintain persistent VPN connectivity for supported Devices and Users, as an extension of the Firewall and VPN Remote Access services described in the Managed Security Service section, using third-party VPN tools and configurations identified in the Order.
- **Block at First Sight**
  Provider will enable and manage advanced malware and file reputation features available in supported security platforms (such as Microsoft Defender or other tools identified in the Order) so that suspicious files can be blocked upon first detection, in coordination with the Security Operations Center and Anti-malware services, subject to those platforms' capabilities.
- **Self Service Password Reset**
  Provider will configure and help administer supported self-service password reset functionality (for example, in Microsoft Entra ID / Active Directory or similar platforms) for eligible Users, with Users managing their own password changes and recoveries in accordance with configured policies and the underlying platform's capabilities.
- **Ransomware Recovery Planning**
  Provider will work with Client to develop or refine documented procedures for responding to and recovering from ransomware incidents, referencing the Data Backup and Disaster Recovery Service and Security Operations Center capabilities described in this Schedule, but does not guarantee that all ransomware attacks can be prevented or that all affected data can be recovered.
- **Enhanced Data Loss Prevention**
  Provider will implement more advanced or granular DLP policies and controls than those included in the Business Plan, including, where applicable, Microsoft 365 DLP and related tools referenced in this Schedule, for the locations and data types identified in the Order, subject to the technical and licensing limitations of the underlying platforms.
- **Privileged Identity Management (PIM)**
  Provider will assist with configuring and managing just-in-time and controlled access for privileged accounts within supported identity and cloud platforms (such as Microsoft Entra ID or other tools identified in the Order), in alignment with the Managed Security Service section and subject to platform capabilities and licensing.
- **Enhanced Audit Reporting**
  Provider will enable and generate more detailed or customized security and compliance reports using log data from Security Log Management, SIEM, and supported platforms (such as Microsoft 365), as permitted by those tools and the Order, recognizing that reporting is limited to data actually collected and retained by the relevant systems.

© Scott & Scott, LLP

- **Advanced ediscovery**
  Provider will assist with configuring and operating advanced eDiscovery features in supported platforms (such as Microsoft 365), including search, hold, and export of data for legal or compliance purposes as requested by Client, consistent with the applicable Third-Party Service Provider terms and technical limitations, while legal strategy and determinations remain Client's responsibility.
- **Sensitivity Labeling**
  Provider will help configure and manage data classification labels and related protection policies in supported platforms (such as Microsoft 365 Information Protection) so Client data can be tagged and handled according to its sensitivity level, subject to the features and licensing detailed in the Order.
- **Support For Microsoft Defender, Intune, Sentinal**
  Provider will implement, configure, and reasonably manage Microsoft Defender, Microsoft Intune, and Microsoft Sentinel (or equivalent Microsoft security and management tools) for in-scope Users and Devices, consistent with the Managed Security Service, Security Operations Center, and Desktop Monitoring and Management descriptions and the Microsoft licensing and technical limitations set forth or referenced in the Order.

MANAGED WORKSTATION

Desktop Monitoring and Management – Provider will perform desktop monitoring and management including, alert monitoring & management of desktops, prioritization of alerts to identify high-priority incidents, remote remediation services as needed, periodic firmware updates as required by manufacturer, and periodic reporting and performance tuning. The Service Fee does not include hardware replacement or new hardware installations.

Help Desk Services – Provider will provide help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control desktops to support employees. Unless otherwise included in an order, all help desk services will include unlimited remote support as required.

On-site Support - Upon request and subject to the limitations identified in the Order, for Services that are within the scope of this Service Attachment, Provider will also deliver support Services on-site at your location during normal business hours. For on-site support that is not included in the Order, Client will pay Provider's then-prevailing hourly rate.

Core Security Services – Provider will include in its services monthly Microsoft patch management, antivirus software and management, and remote software installations. Core Security Services also includes new / terminated employee setup and configuration.

Problem Management Services - Provider will undertake problem management as soon as the Provider's monitoring staff becomes aware of an incident. All incidents, with status or resolution, will be documented by posting updates to the Problem (Incident) Ticket Tracking System assigned to Client ("Problem Tickets").

Vendor Management – Provider will assist with vendor selection, relationship management, KPI monitoring, SLA adherence, contract negotiation, issue resolution, and risk assessment to support vendor collaboration, risk mitigation, and optimized operational and cost outcomes.

MANAGED SECURITY SERVICE

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and

© Scott & Scott, LLP

their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms of use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Firewall and VPN Remote Access – Provider will install and configure firewall traffic policies, apply updated firmware when applicable, and configure changes when needed. With respect to client remote access, Provider will configure virtual private network ("VPN") services for remote access by authorized Client users.

Network Management – Provider will configure and manage routers and switches for secure Internet access and network segmentation based on applicable compliance requirements via the use of dedicated virtual local area networks ("VLAN") for defined use cases such as workstations and printers, phones, guest wireless, servers, and IoT devices.

Spam Prevention - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

Intelligent Antivirus – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.

DNS Filtering - detects and blocks malicious DNS requests at the network edge for onsite users.

Anti-malware - Provider will provide and install anti-malware software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

Client-Side DNS Filtering - Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems. The DNS filtering is designed to detect and block malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices and to protect laptops while away from the corporate network.

Multi-Factor Authentication Services / Password Credential Management Services – Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

© Scott & Scott, LLP

AD HOC SERVICES

Server Monitoring and Management – Provider will perform server monitoring and management including, alert monitoring and management of servers, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed, and backup software monitoring and management. The Service Fee does not include major hardware / software upgrades or replacements or new server installations.

Security Awareness Training & Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Security Risk Assessment

- Malware and Vulnerability Review – Using one or more tools to determine the existence of malware or vulnerabilities.
- Personally Identifiable Information ("PII") – Review practices related to PII, including location, treatment, and risk mitigation.
- Report – Provider's findings will be included in a Risk Assessment Report.

Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

Application Control – Provides the ability to allow, block, or restrict access to applications based on a user's department, job function, and time of day.

Remote Access - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

APT Blocker - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.

Data Loss Prevention – works to enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP.

Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.

Security Operations Center – The Services include:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.

© Scott & Scott, LLP

- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.

Security Log Management – Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

Security Incident Event Management (SIEM) Services supported by SOC – Provider will deploy SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well.

DATA BACKUP AND DISASTER RECOVERY SERVICE

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

Local Backups - Using customer provider hardware and software (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance and notify Client of backup failures. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

Remote Backups - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

Cloud Backup - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order.

Disaster Recovery - Provider will work with Client to develop a comprehensive disaster-recovery plan that incorporates the Services to be delivered under this Service Attachment.

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

FILE BACKUP AND RECOVERY

Provider will create, monitor, and modify up to the number of file backup jobs listed in the Order. Provider will also notify Client by email of backup drive failures and corrective actions.

© Scott & Scott, LLP

Upon request, Provider will remotely restore files, subject to the number of operations listed in the Order.

CLOUD AND HOSTING SERVICES

Public Cloud - Provider will move all Client's data to a cloud computing platform, allow Client to have access to data from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

Hybrid Cloud - Provider will move some of Client's data to a cloud computing platform, and upon Client's request, place a server on premises at Client's location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider's firewall with the public internet (the "Demarcation Point"). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Private Cloud or Software Subscriptions - Provider will maintain all Client's data on premise at Client's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

CYBER TRAINING SERVICES

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals
- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time

© Scott & Scott, LLP

- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

VOIP AND COLLABORATION SERVICES

Provider will deliver the Voice over Internet Protocol ("VoIP") and associated telephony and collaboration services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

The VoIP Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the VoIP Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those third-party vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

Network cabling, conduit, electrical, rack space, and any other required construction or trenching are additional charges and not included with the Service.

**Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.

© Scott & Scott, LLP