Effective March 16, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

ONE82 IT MANAGED SERVICES POC 2026

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.

Accurate System Assessment (ASA) – Provider will perform its proprietary ASA assessment for the client on an as needed basis.

Server Monitoring - Provider will perform remote server monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time, at the discretion of the Provider, and without notice. Server Monitoring is limited to the Server or Servers listed on the Order.

Network Monitoring - Provider will perform remote network monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time, at the discretion of the Provider, and without notice. Network Monitoring is limited to the Network Device or Devices listed on the Order.

Workstation Monitoring - Provider will perform remote workstation monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything, and does not monitor all the time. Provider modifies how it monitors from time to time and at the discretion of the Provider. Workstation Monitoring is limited to the Workstation or Workstations listed on the Order.

Cloud And Hosting Monitoring - Provider will perform remote Cloud and Hosting monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time and at the discretion of the Provider. Cloud and Hosting Monitoring is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Monitoring for those assets are covered under their respective sections. This Cloud and Hosting Monitoring subsection applies only to Cloud And Hosting assets that do not fall under these asset types.

Workstation Optimization - Provider will perform remote workstation optimization using Provider's own Provider defined optimization routines. Provider does not optimize everything and does not optimize all the time. Provider modifies its optimization routines and schedules from time to time, at the discretion of the Provider, and without notice. Workstation Optimization is limited to the Workstation or Workstations listed on the Order.

Cloud And Hosting Optimization - Provider will perform remote Cloud and Hosting optimization, including prioritization of optimization tasks to ensure high-priority operations are

addressed. Provider does not optimize everything and does not optimize all the time. Provider modifies how it optimizes from time to time and at the discretion of the Provider. Cloud And Hosting Optimization is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Optimization for those assets are covered under their respective sections. This Cloud and Hosting Optimization subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

Workstation Patching And Updating - Provider will perform remote workstation operating system patching and updating, and workstation application and software patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all applications and software. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Workstation Patching and Updating is limited to the Workstation or Workstations listed on the Order.

Server Patching And Updating - Provider will perform remote server operating system patching and updating, and server application and software patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all applications and software. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Server Patching And Updating is limited to the Server or Servers listed on the Order.

Network Device Patching And Updating - Provider will perform remote network device operating system patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Network Device Patching And Updating is limited to the Network Device or Devices listed on the Order.

Cloud And Hosting Patching And Updating - Provider will perform remote Cloud and Hosting patching and updating, including prioritization of patching tasks to identify high-priority updates. Provider does not patch or update everything and does not patch or update all the time. Provider modifies how it patches and updates from time to time and at the discretion of the Provider. Cloud And Hosting patching and updating is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the patching and updating for those assets are covered under their respective sections. This Cloud and Hosting patching and updating subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

POC Help Desk Services – Provider will provide remote POC help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees. Unless otherwise included in an Order, all help desk services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Help Desk

© Scott & Scott, LLP

Services does not include any training. Client is required to utilize Provider's ticketing system for all POC Help Desk Services. POC Help Desk Services is limited to a single user that is specified by Client, and Client cannot change the client contact more than one time per month. POC Help Desk Services is limited to the devices listed on the Order.

Software Installs For Workstations – Provider will provide remote Software Installs For Workstations services via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees. Unless otherwise included in an Order, all Software Installs For Workstations services will include remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Software Installs For Workstations is limited to installations for up to one (1) to three (3) workstations. Client is required to utilize Provider's ticketing system for all support. Software Installs For Workstations is limited to the users and devices and software listed on the Order.

Technical Support For Servers – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control servers to provide support. Unless otherwise included in an Order, all Technical Support For Servers services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support For Servers does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support For Servers. Technical Support For Servers is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Servers is limited to the users and devices listed on the Order.

Technical Support For Network Devices – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control network devices to provide support. Unless otherwise included in an Order, all Technical Support For Network Devices services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support For Network Devices does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support For Network Devices. Technical Support For Network Devices is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Network Devices is limited to the users and devices listed on the Order.

Technical Support For Cloud And Hosting Services - Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control Cloud and Hosting assets to provide support. Unless otherwise included in an Order, all Technical Support for Cloud And Hosting Services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support for Cloud and Hosting Services does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support for Cloud and Hosting Services. Technical Support for Cloud and Hosting Services is limited to assisting to restore the Cloud and Hosting assets to their normal operating condition. Technical Support for Cloud and Hosting Services is limited to the cloud and hosting assets, users, and devices listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Technical Support for those assets are covered under their respective sections. This Technical Support for Cloud and Hosting Services subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

Emergency Technical Support For Servers – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control servers to provide support. Unless otherwise included in an Order, all Emergency Technical Support For Servers

© Scott & Scott, LLP

services will include unlimited remote support as required. Emergency Technical Support For is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support For Servers. Emergency Technical Support For Servers is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Servers is limited to the users and devices listed on the Order.

Emergency Technical Support For Routers And Firewalls – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control routers and firewalls to provide support. Unless otherwise included in an Order, all Emergency Technical Support For Routers And Firewalls services will include unlimited remote support as required. Emergency Technical Support For is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support For Routers And Firewalls. Emergency Technical Support For Routers And Firewalls is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Routers And Firewalls is limited to the users and devices listed on the Order.

Emergency Technical Support for Cloud and Hosting Services - Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control Cloud and Hosting assets to provide support. Unless otherwise included in an Order, all Emergency Technical Support for Cloud and Hosting Services will include unlimited remote support as required. Emergency Technical Support for Cloud and Hosting Services is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support for Cloud and Hosting Services. Emergency Technical Support for Cloud and Hosting Services is limited to assisting to restore the Cloud and Hosting assets to their normal operating condition. Emergency Technical Support for Cloud and Hosting Services is limited to the cloud and hosting assets, users, and devices listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Technical Support for those assets are covered under their respective sections. This Emergency Technical Support for Cloud and Hosting Services subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

User Management Services – Provider will include in its services remote new employee provisioning and terminated employee deprovisioning. Provisioning of new employees is limited to user account provisioning in the devices and systems that are listed on the Order, excluding workstations. For provisioning of workstations, including new or existing workstations, Client will pay Provider's then-prevailing hourly rate. Deprovisioning of terminated employees is limited to the user accounts in the systems and devices that are listed on the Order.

If Client requests Provider decommission workstations for any reason, Provider will perform a complete computer reset of the workstation. Provider will not back up any data prior to the requested deprovisioning. **CLIENT UNDERSTANDS THAT ALL DATA WILL BE IRRETRIEVABLY DELETED PERMANENTLY AND AGREES TO HOLD PROVIDER HARMLESS FOR ANY LOSS OR DAMAGES RESULTING FROM REQUESTED DECOMMISSIONING OF WORKSTATIONS.**

© Scott & Scott, LLP

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

ONE82 IT MANAGED SERVICES 2026

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.

ONE82 IT MANAGED SERVICES 2026 includes all the services listed under ONE82 IT MANAGED SERVICES POC 2026 plus:

Help Desk Services – Provider will provide remote help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees. Unless otherwise included in an Order, all help desk services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Help Desk Services does not include any training. Client is required to utilize Provider's ticketing system for all help desk support. Help Desk Services is limited to the users and devices listed on the Order.

On-site Support – If included in an Order and if Provider deems it necessary in its sole discretion , 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.

Application and Contract Visibility - Provider will make available an application and contract visibility service. This service provides Client with centralized visibility into software subscriptions, contracts, renewals, and related spend information through a third-party, web-based platform, and is intended to assist Client in understanding technology usage and identifying potential overspend; however, the service is provided on an availability basis only, Client is solely responsible for entering, maintaining, and managing all data within the platform, Provider does not guarantee accuracy, completeness, alerts, notifications, identification of overspend, or cost savings, and Provider is not responsible for missed renewals, missed notifications, incorrect or incomplete data, or any resulting charges, losses, or business impacts.

Cloud Print Management - Provider will make available a cloud-based print management service limited to the devices listed on the applicable Order. This service is intended to support centralized management and visibility of Client printing environments through a third-party, software-as-a-service platform; however, the service is provided on an availability basis only, Provider does not guarantee availability, performance, compatibility, security outcomes, or cost savings, and Provider is not responsible for print failures, missed jobs, configuration issues, vendor limitations, data loss, or any resulting business interruption, costs, or damages related to Client printing activities.

Acceptable Use Policy Implementation and Management - Provider will make available a set of Acceptable Use Policy templates for Client use, which Client may modify and tailor at its sole discretion and in consultation with its own legal counsel. Provider is not responsible for the content, quality, legality, enforceability, or suitability of any Acceptable Use Policies, whether

© Scott & Scott, LLP

provided as templates or modified by Client. Upon receipt of Client's finalized policies, Provider will make the policies available through Provider's unITy portal and may assign employees listed on the applicable Order a requirement to review the policies through an acknowledgment course for record-keeping purposes only; however, Provider makes no representation that such acknowledgment constitutes a binding agreement, employment contract, or legal enforcement mechanism, Provider is not responsible for ensuring employee participation or compliance, reporting visibility is provided for Client convenience only, and Client retains sole responsibility for policy enforcement, employee management, and compliance oversight.

ONE82 MANAGED SECURITY SERVICES 2026

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.

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 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 or 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. The Managed Security Services take a significant amount of time to implement, configure, and optimize. The Managed Security Services activation process usually takes at least one hundred and twenty (120) days. Provider does not consider the Managed Security Services fully activated until after one hundred twenty (120) days AND when Provider notifies the client that the Managed Security Services are fully activated. Managed Security Services are not fully activated until Provider notifies Client in writing. Charges for the Managed Security Services start on the effective date of the Order. Provider is not a replacement for Cybersecurity insurance. Provider requires client to purchase Cybersecurity insurance and have it in effect within one hundred twenty (120) days after the effective date of the Order. Client is required to be covered under Cybersecurity insurance throughout the duration of the service term as written on the Order. Provider will request a copy of Client's Cybersecurity policy from time to time and as needed, and Client will provide a copy to Provider within seven (7) business days. Client agrees, at Client's sole expense, to purchase and maintain a Microsoft Global Secure Access license, or equivalent solution at Provider's sole discretion, for each user in Client's Microsoft tenant for the duration of the Managed Security Services term, and Client authorizes Provider, in the event required licenses are not already in place or a licensing gap is identified, to procure such licenses on Client's behalf, and Provider shall have no obligation to deliver Services that depend on such licensing if Client fails to do so.

Anti-Virus (AV) - Provider will provide and/or manage existing Anti-Virus software of Provider's choosing for each compatible Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware,

© Scott & Scott, LLP

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.

Endpoint Detection and Response (EDR) – Provider will provide and install Endpoint Detection and Response software of Provider's choosing for each compatible 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.

Network Detection and Response (NDR) – Provider will provide and install Network Detection and Response software of Provider's choosing for each compatible 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.

SaaS Detection and Response (SAASDR) – Provider will provide and configure SaaS Detection and Response service and/or software of Provider's choosing for each compatible SaaS service covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from business email compromise, 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.

Endpoint Access Control / Zero Trust (EAC) – Provider will provide and install Endpoint Access Control software of Provider's choosing for each compatible Device covered by the Order. Provides the ability to allow, block, or restrict access to applications and storage devices based on a user's group and time of day.

Endpoint Internet Access Control And Protection (EIACP) - Provider will provide and/or manage software of Provider's choosing for each compatible Device covered by the Order, that helps control the web and application traffic between devices and the Internet. Provider makes best efforts to provide filtering and inspection for most traffic, but some traffic and applications may not be covered due to compatibility and other quality and performance reasons.

Endpoint Zero Trust Network Access (EZTNA) – Provider will provide and install Endpoint Zero Trust Network Access software of Provider's choosing for each compatible Device covered by the Order. Leverages the deny by default design and integrates with identity to only allow a

© Scott & Scott, LLP

user to access specific applications or services. Provider only configures and enables EZTNA upon Client's request, and should Client choose to request enabling EZTNA, Client must request the enabling after the Order.

Browser Security and Access Controls – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using browser security, monitoring, and access control software and/or services of Provider's choosing. The service provides browser-level security controls and visibility for web and SaaS application access, including policy enforcement, activity monitoring, and protections designed to reduce risks associated with phishing, malware, and unsafe web content. Browser Security and Access Controls is limited to the users, browsers, and devices listed on the Order, and Provider does not guarantee prevention of all malicious activity or unauthorized access. Provider does not control third-party websites, SaaS platforms, or internet content accessed by users and does not monitor all browser activity at all times. Provider may modify configurations, policies, features, or enforcement methods from time to time at its discretion and without notice. This service does not include endpoint protection beyond the browser, identity management, security awareness training, or incident response services unless expressly included in the Order.

Security Awareness Training & Phishing Simulations (SAT & PS) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. 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.

Dark Web Monitoring (DWM) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Unless otherwise specified on the Order, Dark Web Monitoring only covers a single client domain for all the users. Unless otherwise specified on the order, the Service will scan for Dark Web information once per month.

Incident Response Assistance - Provider will assist Client in the hours immediately following a data breach to assist in identifying the likely source of the breach and to assist client's Cybersecurity Insurance Incident Response team to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the one (1) hour 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. Provider is not an Incident Response firm. Provider does not provide incident response services. Provider will provide best effort to support Client's Incident Response team which is either provided by Client's Cybersecurity Insurance provider and/or the Client's Incident Response team. 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.

Desired State Management for Microsoft 365 (DSMM365) – Provider will include in its services Desired State Management for each Microsoft 365 Tenant covered by the Order, using software and/or services of Provider's choosing. Desired State Management is limited to third-party scope of management of Microsoft 365 tenants. Desired State Management does not manage and monitor all Microsoft 365 configuration settings.

© Scott & Scott, LLP

Spam & Phishing Prevention – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Real-time, continuous, and highly reliable protection from spam and phishing attempts.

Email Encryption – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using email encryption software and/or services of Provider's choosing. The service provides outbound encrypted email messaging and secure file transfer functionality and enables users to send encrypted email and securely transfer files using standard email clients without the requirement to install additional applications, plugins, or client-side software, with encrypted messages and files protected using industry-standard encryption. Email Encryption is limited to the users, email accounts, and domains listed on the Order, and Provider does not guarantee that all messages or files will be encrypted in all circumstances and does not monitor or control user behavior. Provider may modify configurations, features, or deployment methods from time to time at its discretion and without notice. This service does not include data retention management, legal discovery services, compliance archiving, user training, or incident response services unless expressly included in the Order.

Email Authentication and DMARC Management – Provider will acquire and will assign an appropriate number of licenses to support each domain covered by the Order, using email authentication, monitoring, and DMARC management software and/or services of Provider's choosing. The service provides domain-level visibility and reporting for email authentication technologies including DMARC, SPF, and DKIM, and may include tools to assist with monitoring, analysis, and configuration of related DNS records to help identify unauthorized email sources and improve email deliverability. Email Authentication and DMARC Management is limited to the domains listed on the Order, and Provider does not guarantee email delivery, authentication outcomes, or protection from spoofing, phishing, or other email-based threats. Provider does not control third-party email systems or sending infrastructure and does not monitor all email traffic. Provider may modify configurations, tools, processes, or features from time to time at its discretion and without notice. This service does not include remediation of third-party systems, ongoing DNS management outside the scope of the service, legal or regulatory compliance guarantees, user training, or incident response services unless expressly included in the Order.

Secure File Transfer – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using secure file transfer software and/or services of Provider's choosing. The service provides encrypted file transfer functionality that allows users and external parties to securely send and receive files and messages without the requirement to create accounts, install applications, or use client-side software, with shared files and messages protected using industry-standard encryption. Secure File Transfer is limited to the users, share links, and file transfer functionality associated with the users listed on the Order, and Provider does not guarantee the delivery, availability, or retention of files or messages and does not monitor or control the content transmitted through the service. Provider may modify configurations, features, limits, or access methods from time to time at its discretion and without notice. This service does not include data retention management, compliance archiving, legal discovery services, user training, or incident response services unless expressly included in the Order.

© Scott & Scott, LLP

Provider Remote Access For Security - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Provider Remote Access For Security is solely for the use of Provider. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

One82 unITy Web Portal – Provider, through its Third-Party Service Providers, and upon Client's request, will provide the One82 unITy Web Portal service to Client as a convenience service for each user covered by the Order. The One82 unITy Web Portal service provides Client with access to ticket information from Provider. While the One82 unITy Web Portal service may have other features available to Client, Provider has the right to change all of the features and functionality at any time and without any notice. Provider maintains all rights to the configuration, information, and data on the One82 unITy Web Portal. At any time Provider may discontinue the One82 unITy Web Portal service without affecting any of the terms and conditions of the Order, and including the fees associated on the Order.

SECURITY SERVICES ADD-ONS 2026

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.

Dark Web Monitoring For Personal (DWMFP) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Unless otherwise specified on the Order, Dark Web Monitoring only covers the email addresses specified on the Order. Unless otherwise specified on the order, the Service will scan for Dark Web information once per month.

SASE Tunnel – Provider will provide and configure SASE Tunnel of Provider's choosing for each Device covered by the Order. SASE Tunnel service provides a VPN connection from Client's site firewall to the SASE network.

Network Discovery – Provider will perform a scan of Client's networks and devices to generate an inventory of the discoverable nodes on your network. Unless otherwise specified on the Order, Network Discovery is performed on an as needed basis or if Client requests it. For Network Discovery that is not included in the Order, Provider will prepare a separate Order for Project Services that will specify what the charges will be for such assistance.

Security Risk Assessment - Provider will, or will hire a third-party to, perform a scan of Client's networks and devices to help Client determine the Client's security posture. Unless otherwise specified in the Order, Security Risk Assessment is performed on an as needed basis or if Client requests it. For Security Risk Assessment that is not included in the Order, Provider will prepare a separate Order for Project Services that will specify what the charges will be for such assistance.

Security Monitoring and Event Management Services Supported by SOC–

Provider will include in its services a comprehensive security monitoring and event management solution, selected by Provider, for each compatible device covered by the Order. Additionally, Provider may extend these services to compatible cloud services covered by the Order. These security monitoring services are exclusively utilized by Provider's and/or Partner's third-party

© Scott & Scott, LLP

Security Operations Center (SOC) for security monitoring and reporting purposes. Unless otherwise specified in an Order, these services are limited to a 7-day data retention period.

ONE82 MANAGED AI SERVICES 2026

The Services to be performed for Client by Provider are set forth in the Order. Provider may make available managed artificial intelligence related services intended to assist Client in evaluating, planning, and understanding potential AI usage within Client's organization. These services are advisory in nature only and do not constitute legal, regulatory, compliance, financial, or operational advice, and Provider does not guarantee outcomes, results, adoption success, or business impact arising from any AI-related services.

AI Readiness and Adoption Assessment - Provider will perform an assessment of Client's artificial intelligence readiness and adoption to assist Client in understanding its current state and potential considerations related to AI usage. Unless otherwise specified on the applicable Order, this assessment is intended to be performed once per year; however, Client acknowledges that failure to perform the assessment within any specific timeframe, including annually, shall not constitute a failure to deliver Services or a breach of the Agreement, and any additional assessments may be performed at Provider's sole discretion. Provider does not guarantee recommendations, implementation feasibility, compliance, or results, and Client remains solely responsible for all decisions, actions, and use of any information provided as part of the assessment.

AI Acceptable Use Policy Implementation and Management - Provider may make available a set of artificial intelligence acceptable use policy templates for Client use, which Client may modify and tailor at its sole discretion and in consultation with its own legal counsel. Provider is not responsible for the content, quality, legality, enforceability, accuracy, or suitability of any AI acceptable use policies, whether provided as templates or modified by Client. Upon receipt of Client's finalized policies, Provider will make the policies available through Provider's unITy portal and may assign users listed on the applicable Order a requirement to review the policies through an acknowledgment course for record-keeping purposes only; however, Provider makes no representation that such acknowledgment constitutes a binding agreement, employment contract, or legal enforcement mechanism, Provider is not responsible for ensuring user participation or compliance, reporting visibility is provided for Client convenience only, and Client retains sole responsibility for policy enforcement, employee management, compliance oversight, and any risks associated with AI usage.

AI Training For Users - Provider may make available artificial intelligence training content through Provider's unITy portal for users listed on the applicable Order. Provider's role is limited to making training courses available and providing reporting visibility regarding completion status; Provider is not responsible for ensuring that Client's employees complete any training, and Client retains sole responsibility for managing employee participation, enforcement, and follow-up. Reporting is provided for Client convenience only, and Client acknowledges that employee completion or non-completion of training does not transfer responsibility, liability, or compliance obligations to Provider.

AI Usage Control and Enforcement - Provider may make available an AI usage control service intended to assist Client in restricting access to artificial intelligence services that are not

© Scott & Scott, LLP

authorized by Client. When included on the applicable Order, this service applies only to the users and devices listed on the Order and is intended to allow Client to define and control which AI services may be accessed; however, Provider does not guarantee complete enforcement, blocking, detection, or prevention of unauthorized AI usage, Provider is not responsible for user behavior, circumvention attempts, third-party limitations, or changes in AI services, and Client retains sole responsibility for defining authorized AI usage, managing internal policies, and addressing any risks, compliance obligations, or impacts arising from employee use of artificial intelligence.

ONE82 IT MANAGED SERVICES POC 2024

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.

Accurate System Assessment (ASA) – Provider will perform its proprietary ASA assessment for the client on an as needed basis.

Server Monitoring - Provider will perform remote server monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time, at the discretion of the Provider, and without notice. Server Monitoring is limited to the Server or Servers listed on the Order.

Network Monitoring - Provider will perform remote network monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time, at the discretion of the Provider, and without notice. Network Monitoring is limited to the Network Device or Devices listed on the Order.

Workstation Monitoring - Provider will perform remote workstation monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything, and does not monitor all the time. Provider modifies how it monitors from time to time and at the discretion of the Provider. Workstation Monitoring is limited to the Workstation or Workstations listed on the Order.

Cloud And Hosting Monitoring - Provider will perform remote Cloud and Hosting monitoring, including prioritization of alerts to identify high-priority incidents. Provider does not monitor everything and does not monitor all the time. Provider modifies how it monitors from time to time and at the discretion of the Provider. Cloud and Hosting Monitoring is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Monitoring for those assets are covered under their respective sections. This Cloud and Hosting Monitoring subsection applies only to Cloud And Hosting assets that do not fall under these asset types.

Workstation Optimization - Provider will perform remote workstation optimization using Provider's own Provider defined optimization routines. Provider does not optimize everything and does not optimize all the time. Provider modifies its optimization routines and schedules from time to time, at the discretion of the Provider, and without notice. Workstation Optimization is limited to the Workstation or Workstations listed on the Order.

© Scott & Scott, LLP

Cloud And Hosting Optimization - Provider will perform remote Cloud and Hosting optimization, including prioritization of optimization tasks to ensure high-priority operations are addressed. Provider does not optimize everything and does not optimize all the time. Provider modifies how it optimizes from time to time and at the discretion of the Provider. Cloud And Hosting Optimization is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Optimization for those assets are covered under their respective sections. This Cloud and Hosting Optimization subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

Workstation Patching And Updating - Provider will perform remote workstation operating system patching and updating, and workstation application and software patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all applications and software. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Workstation Patching and Updating is limited to the Workstation or Workstations listed on the Order.

Server Patching And Updating - Provider will perform remote server operating system patching and updating, and server application and software patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all applications and software. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Server Patching And Updating is limited to the Server or Servers listed on the Order.

Network Device Patching And Updating - Provider will perform remote network device operating system patching and updating. Provider patches and updates using Provider's own Provider defined updating and patching routines and schedules. Provider does not patch or update everything and does not patch or update all the time. Provider modifies the scope, schedule, methodology, of how it patches and updates from time to time and at the discretion of the Provider. Provider does not patch and update all updates available, and at its sole discretion Provider may exclude certain patches or updates. Network Device Patching And Updating is limited to the Network Device or Devices listed on the Order.

Cloud And Hosting Patching And Updating - Provider will perform remote Cloud and Hosting patching and updating, including prioritization of patching tasks to identify high-priority updates. Provider does not patch or update everything and does not patch or update all the time. Provider modifies how it patches and updates from time to time and at the discretion of the Provider. Cloud And Hosting patching and updating is limited to the Cloud and Hosting assets listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the patching and updating for those assets are covered under their respective sections. This Cloud and Hosting patching and updating subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

POC Help Desk Services – Provider will provide remote POC help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees.

© Scott & Scott, LLP

Unless otherwise included in an Order, all help desk services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Help Desk Services does not include any training. Client is required to utilize Provider's ticketing system for all POC Help Desk Services. POC Help Desk Services is limited to a single user that is specified by Client, and Client cannot change the client contact more than one time per month. POC Help Desk Services is limited to the devices listed on the Order.

Software Installs For Workstations – Provider will provide remote Software Installs For Workstations services via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees. Unless otherwise included in an Order, all Software Installs For Workstations services will include remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Software Installs For Workstations is limited to installations for up to one (1) to three (3) workstations. Client is required to utilize Provider's ticketing system for all support. Software Installs For Workstations is limited to the users and devices and software listed on the Order.

Technical Support For Servers – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control servers to provide support. Unless otherwise included in an Order, all Technical Support For Servers services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support For Servers does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support For Servers. Technical Support For Servers is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Servers is limited to the users and devices listed on the Order.

Technical Support For Network Devices – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control network devices to provide support. Unless otherwise included in an Order, all Technical Support For Network Devices services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support For Network Devices does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support For Network Devices. Technical Support For Network Devices is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Network Devices is limited to the users and devices listed on the Order.

Technical Support For Cloud And Hosting Services - Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control Cloud and Hosting assets to provide support. Unless otherwise included in an Order, all Technical Support for Cloud And Hosting Services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Technical Support for Cloud and Hosting Services does not include any training. Client is required to utilize Provider's ticketing system for all Technical Support for Cloud and Hosting Services. Technical Support for Cloud and Hosting Services is limited to assisting to restore the Cloud and Hosting assets to their normal operating condition. Technical Support for Cloud and Hosting Services is limited to the cloud and hosting assets, users, and devices listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Technical Support for those assets are covered under their respective sections. This Technical Support for Cloud and Hosting Services subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

© Scott & Scott, LLP

Emergency Technical Support For Servers – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control servers to provide support. Unless otherwise included in an Order, all Emergency Technical Support For Servers services will include unlimited remote support as required. Emergency Technical Support For is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support For Servers. Emergency Technical Support For Servers is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Servers is limited to the users and devices listed on the Order.

Emergency Technical Support For Routers And Firewalls – Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control routers and firewalls to provide support. Unless otherwise included in an Order, all Emergency Technical Support For Routers And Firewalls services will include unlimited remote support as required. Emergency Technical Support For is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support For Routers And Firewalls. Emergency Technical Support For Routers And Firewalls is limited to assisting to restore the operating system or software back to its normal operating condition. Technical Support For Routers And Firewalls is limited to the users and devices listed on the Order.

Emergency Technical Support for Cloud and Hosting Services - Provider will provide remote technical support via client portal, e-mail, and phone. Provider has the ability to remotely control Cloud and Hosting assets to provide support. Unless otherwise included in an Order, all Emergency Technical Support for Cloud and Hosting Services will include unlimited remote support as required. Emergency Technical Support for Cloud and Hosting Services is limited to emergencies as defined by Provider, and Provider has the right to change the definition of an emergency at any time and without notice. Client is required to utilize Provider's ticketing system for all Emergency Technical Support for Cloud and Hosting Services. Emergency Technical Support for Cloud and Hosting Services is limited to assisting to restore the Cloud and Hosting assets to their normal operating condition. Emergency Technical Support for Cloud and Hosting Services is limited to the cloud and hosting assets, users, and devices listed on the Order. If a Cloud and Hosting asset is a workstation, network device, or server, the Technical Support for those assets are covered under their respective sections. This Emergency Technical Support for Cloud and Hosting Services subsection applies only to Cloud and Hosting assets that do not fall under these asset types.

User Management Services – Provider will include in its services remote new employee provisioning and terminated employee deprovisioning. Provisioning of new employees is limited to user account provisioning in the devices and systems that are listed on the Order, excluding workstations. For provisioning of workstations, including new or existing workstations, Client will pay Provider's then-prevailing hourly rate. Deprovisioning of terminated employees is limited to the user accounts in the systems and devices that are listed on the Order.

If Client requests Provider decommission workstations for any reason, Provider will perform a complete computer reset of the workstation. Provider will not back up any data prior to the requested deprovisioning. **CLIENT UNDERSTANDS THAT ALL DATA WILL BE IRRETRIEVABLY DELETED PERMANENTLY AND AGREES TO HOLD PROVIDER**

© Scott & Scott, LLP

HARMLESS FOR ANY LOSS OR DAMAGES RESULTING FROM REQUESTED DECOMMISSIONING OF WORKSTATIONS.

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

ONE82 IT MANAGED SERVICES 2024

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.

ONE82 IT MANAGED SERVICES 2024 includes all the services listed under ONE82 IT MANAGED SERVICES POC 2024 plus:

Help Desk Services – Provider will provide remote help desk support via client portal, e-mail, and phone. Provider has the ability to remotely control workstations to support employees. Unless otherwise included in an Order, all help desk services will include unlimited remote support as required, between 8am-5pm PST, Mon-Fri, excluding Provider company holidays. Help Desk Services does not include any training. Client is required to utilize Provider's ticketing system for all help desk support. Help Desk Services is limited to the users and devices listed on the Order.

On-site Support – If included in an Order and if Provider deems it necessary in its sole discretion , 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, Client will pay Provider's then-prevailing hourly rate.

ONE82 MANAGED SECURITY SERVICES 2024

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.

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 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 or 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. The Managed Security Services take a significant amount of time to implement, configure, and optimize. The Managed Security Services activation process usually takes at

© Scott & Scott, LLP

least one hundred and twenty (120) days. Provider does not consider the Managed Security Services fully activated until after one hundred twenty (120) days AND when Provider notifies the client that the Managed Security Services are fully activated. Managed Security Services are not fully activated until Provider notifies Client in writing. Charges for the Managed Security Services start on the effective date of the Order. Provider is not a replacement for Cybersecurity insurance. Provider requires client to purchase Cybersecurity insurance and have it in effect within one hundred twenty (120) days after the effective date of the Order. Client is required to be covered under Cybersecurity insurance throughout the duration of the service term as written on the Order. Provider will request a copy of Client's Cybersecurity policy from time to time and as needed, and Client will provide a copy to Provider within seven (7) business days.

Anti-Virus (AV) - Provider will provide and/or manage existing Anti-Virus software of Provider's choosing for each compatible 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.

Endpoint Detection and Response (EDR) – Provider will provide and install Endpoint Detection and Response software of Provider's choosing for each compatible 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.

Network Detection and Response (NDR) – Provider will provide and install Network Detection and Response software of Provider's choosing for each compatible 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.

SaaS Detection and Response (SAASDR) – Provider will provide and configure SaaS Detection and Response service and/or software of Provider's choosing for each compatible SaaS service covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from business email compromise, 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.

© Scott & Scott, LLP

Endpoint Access Control / Zero Trust (EAC) – Provider will provide and install Endpoint Access Control software of Provider's choosing for each compatible Device covered by the Order. Provides the ability to allow, block, or restrict access to applications and storage devices based on a user's group and time of day.

Endpoint Internet Access Control And Protection (EIACP) - Provider will provide and/or manage software of Provider's choosing for each compatible Device covered by the Order, that helps control the web and application traffic between devices and the Internet. Provider makes best efforts to provide filtering and inspection for most traffic, but some traffic and applications may not be covered due to compatibility and other quality and performance reasons.

Endpoint Zero Trust Network Access (EZTNA) – Provider will provide and install Endpoint Zero Trust Network Access software of Provider's choosing for each compatible Device covered by the Order. Leverages the deny by default design and integrates with identity to only allow a user to access specific applications or services. Provider only configures and enables EZTNA upon Client's request, and should Client choose to request enabling EZTNA, Client must request the enabling after the Order.

Security Awareness Training & Phishing Simulations (SAT & PS) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. 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.

Dark Web Monitoring (DWM) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Unless otherwise specified on the Order, Dark Web Monitoring only covers a single client domain for all the users. Unless otherwise specified on the order, the Service will scan for Dark Web information once per month.

Incident Response Assistance - Provider will assist Client in the hours immediately following a data breach to assist in identifying the likely source of the breach and to assist client's Cybersecurity Insurance Incident Response team to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the one (1) hour 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. Provider is not an Incident Response firm. Provider does not provide incident response services. Provider will provide best effort to support Client's Incident Response team which is either provided by Client's Cybersecurity Insurance provider and/or the Client's Incident Response team. 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.

Desired State Management for Microsoft 365 (DSMM365) – Provider will include in its services Desired State Management for each Microsoft 365 Tenant covered by the Order, using software and/or services of Provider's choosing. Desired State Management is limited to third-party scope of management of Microsoft 365 tenants. Desired State Management does not manage and monitor all Microsoft 365 configuration settings.

© Scott & Scott, LLP

Spam & Phishing Prevention – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Real-time, continuous, and highly reliable protection from spam and phishing attempts.

Provider Remote Access For Security - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Provider Remote Access For Security is solely for the use of Provider. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

One82 unITy Web Portal – Provider, through its Third-Party Service Providers, and upon Client's request, will provide the One82 unITy Web Portal service to Client as a convenience service for each user covered by the Order. The One82 unITy Web Portal service provides Client with access to ticket information from Provider. While the One82 unITy Web Portal service may have other features available to Client, Provider has the right to change all of the features and functionality at any time and without any notice. Provider maintains all rights to the configuration, information, and data on the One82 unITy Web Portal. At any time Provider may discontinue the One82 unITy Web Portal service without affecting any of the terms and conditions of the Order, and including the fees associated on the Order.

SECURITY SERVICES ADD-ONS 2024

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.

Dark Web Monitoring For Personal (DWMFP) – Provider will acquire and will assign an appropriate number of licenses to support each user covered by the Order, using software and/or services of Provider's choosing. Unless otherwise specified on the Order, Dark Web Monitoring only covers the email addresses specified on the Order. Unless otherwise specified on the order, the Service will scan for Dark Web information once per month.

SASE Tunnel – Provider will provide and configure SASE Tunnel of Provider's choosing for each Device covered by the Order. SASE Tunnel service provides a VPN connection from Client's site firewall to the SASE network.

Network Discovery – Provider will perform a scan of Client's networks and devices to generate an inventory of the discoverable nodes on your network. Unless otherwise specified on the Order, Network Discovery is performed on an as needed basis or if Client requests it. For Network Discovery that is not included in the Order, Provider will prepare a separate Order for Project Services that will specify what the charges will be for such assistance.

Security Risk Assessment - Provider will, or will hire a third-party to, perform a scan of Client's networks and devices to help Client determine the Client's security posture. Unless otherwise specified in the Order, Security Risk Assessment is performed on an as needed basis or if Client requests it. For Security Risk Assessment that is not included in the Order, Provider will prepare a separate Order for Project Services that will specify what the charges will be for such assistance.

© Scott & Scott, LLP

Security Monitoring and Event Management Services Supported by SOC–

Provider will include in its services a comprehensive security monitoring and event management solution, selected by Provider, for each compatible device covered by the Order. Additionally, Provider may extend these services to compatible cloud services covered by the Order. These security monitoring services are exclusively utilized by Provider's and/or Partner's third-party Security Operations Center (SOC) for security monitoring and reporting purposes. Unless otherwise specified in an Order, these services are limited to a 7-day data retention period.

ONE82 MANAGED BACKUP SERVICES 2024

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.

BCDR – 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 workstation/server software application (the "Application"), encrypted, and then sent to a storage appliance located on the Client's network. Backup data are encrypted, and then sent to a storage server at third-party vendor's data center facility. Using hardware and software provided by the provider, Provider will install and configure backup appliance or appliances and install backup agent or agents on devices covered by the Order. The backup hardware and software are purchased and remains the property of the Provider. The backup hardware and software are manufactured and supported by a third-party of Provider's choosing. Provider will configure local backups to the appliance or appliances, on the basis specified on the Order. Provider will configure backups from the appliance to the third-party cloud datacenter, on the basis specified on the Order. While Provider will make reasonable effort to monitor backups to help ensure that they are running correctly, Provider does not guarantee that Client backups are restorable and functioning correctly.

Microsoft Azure BCDR - 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 workstation/server software application (the "Application"), encrypted, and then sent to an Azure virtual storage appliance or appliances located on the Third-Party Datacenter. Using services and software provided by the provider, Provider will install backup agent or agents on devices covered by the Order. The backup services and software are purchased and remains the property of the Provider. The backup services and software are manufactured and supported by a Third-Party of Provider's choosing. Provider will configure backups to the Third-Party Datacenter, on the basis specified on the Order. While Provider will make reasonable effort to monitor backups to help ensure that they are running correctly, Provider does not guarantee that Client backups are restorable and functioning correctly.

Microsoft Azure Backup - Provider, through its Third-Party Service Providers, will make its best effort to ensure the protection and recovery of Client's information using Microsoft Azure's

© Scott & Scott, LLP

backup system. Data files are backed up via Microsoft Azure's native backup services and then stored in Azure storage within the Client's own Microsoft Azure tenant. Using services and software provided by Provider, Provider will configure backup policies on assets covered by the Order. The backup services and software are provided by Microsoft Azure and remain the property of Microsoft. Provider's role is limited to configuring, monitoring, and providing technical support for the backup services. Unless otherwise requested by the Client, the backup retention schedule is at the discretion of Provider. Backups exceeding the retention schedule will be automatically deleted and cannot be restored. Client fully understands and acknowledges that once backups are deleted after exceeding the retention period, they cannot be recovered. Client takes complete responsibility for ensuring that the retention schedule meets their data preservation needs and accepts all risks associated with data loss.

SaaS Cloud Backup – Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information located on the SaaS Service specified in the Order. Data is backed up via a third-party direct API, encrypted, and then sent to a third-party, encrypted, and then sent to Third-Party server located on the Third-Party Datacenter. The backup services and software are manufactured and supported by a Third-Party of Provider's choosing. If not otherwise specified in the Order, Provider will configure backups to the Third-Party Datacenter, on the basis of once per day. While Provider will make reasonable effort to monitor backups to help ensure that they are running correctly, Provider does not guarantee that Client backups are restorable and functioning correctly.

ONE82 MANAGED CLOUD AND HOSTING SERVICES 2024

Provider will resell Microsoft Azure cloud resources for the Client, including but not limited to Azure Compute, Azure Gateways, Azure Files, Azure SQL Database, and other Microsoft Azure services as specified in the Order.

Tenant Ownership: All Microsoft Azure assets and resources will be deployed and reside within the Client's own Azure tenant. The Client retains full ownership and control over their Azure tenant and associated resources. Provider's role is limited to facilitating the subscription access to the Azure services as outlined in this Agreement.

Billing: Provider will invoice the Client for the resold Azure services based on the pricing structure detailed in the Order. This billing covers the usage of Azure resources and any associated fees for facilitating the subscription.

Setup and Configuration: Provider will handle the processing of the Order to ensure that the Client has subscription access to the specified Microsoft Azure services. Provider does not provide support related to the architecture, configuration, installation, maintenance, or ongoing support of the Azure services.

Support:

- Basic Support - The support provided under this section is limited to processing the Order and ensuring that the Client has active subscription access to the Microsoft Azure services specified in the Order.

© Scott & Scott, LLP

- One82 IT Managed Services - If the Client is subscribed to Provider's IT Managed Services and the Azure resources are added as supported assets on the approved Order, Provider will extend support for these Microsoft Azure resources in accordance with the relevant sections of the IT Managed Services Schedule of Services. Reference the scope of support as defined in the respective service sections.

- One82 Managed Security Services - If the Client is subscribed to Provider's Managed Security Services and the Azure resources are added as supported assets on the approved Order, Provider will extend support for these Microsoft Azure resources in accordance with the relevant sections of the Managed Security Services Schedule of Services. Reference the scope of support as defined in the respective service sections.

- One82 Managed Backup Services - If the Client is subscribed to Provider's Managed Backup Services and the Azure resources are added as supported assets on the approved Order, Provider will extend support for these Microsoft Azure resources in accordance with the relevant sections of the Managed Backup Services Schedule of Services. Reference the scope of support as defined in the respective service sections.

- Exclusions - Architecture, configuration, and installation services are not included in this service or any other service listed in this Schedule of Services. Such services must be obtained through a separate project Order for professional services.

Service Modifications: Provider reserves the right to modify the processes and methodologies used to facilitate the subscription access to Azure services at its sole discretion and without prior notice. Any significant changes that may impact the Client's access to the services will be communicated.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.

© Scott & Scott, LLP