Effective March 8, 2024. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote.

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 Quote, 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 Quote.

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 PERMANETNLY AND AGREES TO HOLD PROVIDER 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 Quote.

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 Client's 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 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 Quote. Client is required to be covered under Cybersecurity insurance throughout the duration of the service term as written on the Quote. 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.

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.

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, will provide the One82 unITy Web Portal service to 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 Quote 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 Quote for Project Services that will specify what the charges will be for such assistance.

Security Incident Event Management (SIEM) Services supported by SOC – Provider will include in its services Security Information and Event Management (SIEM), of Provider's choosing, for each compatible Device covered by the Order. Also, Provider may include SIEM for compatible cloud services covered by the Order. SIEM service is solely used by Provider's and/or Partner's third party Security Operations Center (SOC) for security monitoring and reporting. Unless otherwise included in an Order, SIEM services are limited to 7-day retention.

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.

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.

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.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.