Business System Solutions, Inc.

Services Statement

Hello, and thank you for entrusting Business System Solutions, Inc. ("BSS") to provide you with professional information technology services. This Services Statement (this "Agreement") governs BSS' business relationship with you, so please read this document carefully and keep a copy for your records.

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

This Services Statement is BSS' "owner's manual" that generally describes all managed services provided or facilitated by BSS; however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). Activities or items that are not specifically described in the Quote will be out of scope ("Out of Scope") and will not be included unless otherwise agreed to by BSS in writing.

This Services Statement contains important provisions pertaining to the auto-renewal of the Services your Quote, as well as fee increases that may occur from time-to-time. Please read this Services Statement carefully and keep a copy for your records.

Onboarding Services

The Onboarding Quote is required and contingent upon the acceptance of the Managed IT Services Agreement Quote, which will be provided as a separate Quote. Onboarding services will begin on or after the Commencement Date.

Ongoing/Recurring Services

Ongoing/recurring services, Manaaged Services "Agreement", are services that are provided to you on an ongoing basis and, unless otherwise indicated in the Quote, are billed to you monthly. Ongoing services will begin on the Commencement Date or as agreed upon by BSS and Client. Onboarding may begin prior to, on, or after the Commencement Date.

Managed Services

The following Services, if listed in the Quote, will be provided to you.

1-MANAGED SITE SUPPORT MAY INCLUDE:	
Remote/Onsite Labor Support Requests Included *(Pro-Security plan)*	• Technical resources will be assigned as available and with the appropriate experience level required to resolve the issue. If necessary, other resources will assist or the ticket will be escalated to an alternative resource. • All Proactive Support is included. • All Client support requested incidents and service/user requests are included. • **BSS recommendations and projects will be quoted separately.**
Remote only Labor Support included / Onsite Requests Billed Hourly *(Remote Advantage plan)*	• Technical resources will be assigned as available and with the appropriate experience level required to resolve the issue. If necessary, other resources will assist or the ticket will be escalated to an alternative resource. • All Proactive Support is included. • All Client requested remote support for incidents and service/user requests are included. • All Client on site requested incidents and service/user requests are billable at the rated stated in the Quote. • **BSS recommendations and projects will be quoted separately.**
Remote/Onsite Labor Support Requests Billed Hourly *(Basic plan)*	• Technical resources will be assigned as available and with the appropriate experience level required to resolve the issue. If necessary, other resources will assist or the ticket will be escalated to an alternative resource. • All Proactive Support is included. • All Client requested incidents and service/user requests are billable at the rated stated in the Quote. • **BSS recommendations and projects will be quoted separately.**

Managed Site Support: Remote Monitoring and Management	• Software agents are installed on Covered Equipment (defined below) report status and events on a 24x7 basis. • Alerts are generated and responded to in accordance with the Service Levels described below. • Basic routine system maintenance and optimization are performed. • Secure remote access software will be installed for BSS access to Covered Equipment.
Managed Site Support: Software Updates & Patches	• Includes services for the following: Vendor-supported Windows operating systems on laptops, desktops, and servers; vendor-supported select peripherals and networking equipment; common third-party applications such as Adobe Reader, Chrome, Firefox, etc. • Deploy, manage, and monitor the installation of approved feature updates, minor updates, security updates, critical security patches, and firmware updates as deemed necessary on all applicable managed hardware. • Known problematic updates and patches are prevented from being installed. BSS will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third-party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. BSS will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. BSS reserves the right, but not the obligation, to refrain from installing a Patch if BSS is aware of technical problems caused by a Patch, or BSS believes that a Patch may render the Environment, or any portion of the Environment, unstable.
Managed Site Support: Proactive Support	Along with automatically generated alerts, tickets are initiated by BSS with tasks to perform proactive monthly maintenance and review to ensure all computers, servers, and network equipment settings align with BSS best practices. Examples include firmware updates, review of firewall configuration, audits of DNS web filtering, virtual infrastructure health checks.
Managed Site Support: Monthly Reports	• Servers, workstations, and user counts. • Office 365 license counts. • Inventory list for servers and workstations. • List of users with Microsoft 365 email. • Additional information as it is available.
Managed Site Support: Client Payment Portal	• Client payment portal with access to current and past invoices. • Credit or debit card or ACH payment options. • Automatically pay recurring agreements. • Client information is protected in a 100% PCI compliant payment vault. • If a debit or credit card is used there may be a surcharge.
Managed Site Support: Account Management	An account manager will be assigned to Client. The account manager will lead the Business Review Meetings and will be the Client point of contact for customer service-related and technology questions. Listed below are typical situations when Client will contact Client's account manager: • New projects such as building moves, new applications, compliance requirements, new technology equipment, etc. • General, high-level technology questions. • Questions on invoices. • Questions on service. Suggestions and advice rendered to Client are provided in accordance with relevant industry practices, based on Client's specific needs and BSS' opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, BSS is not endorsing any particular manufacturer or service provider. NOTE: Technical Support requests should go to support@bssconsulting.com.
Firewall Management	• Manage firewall hardware, licensing, and current vendor support. • Configure firewall to only allow valid incoming traffic. • Perform firmware, security, and other updates as needed. • Administer firewall when changes are required for new applications or functions. • Setup VPN access according to best practice standards.

Server Support	• Diagnose and coordinate the repair of server hardware (parts are the responsibility of the Client unless covered as HaaS Equipment). • Maintain storage health and utilization. • Monitor for healthy server services (including Active Directory, DHCP, DNS, SQL, etc.). • Advise on proper Microsoft server licensing compliance. • Manage the Active Directory environment including user creation, updates and removal, Group Policy, and security groups and user permissions.
Shared Computer Support (no specific user)	• Provide support for computers such as point of sale (POS), CNC, kiosks, shared, and special-use computers that are not designated to a particular user. • If hardware and/or software are provided by a third-party vendor, it must be covered under the vendor's warranty, licensing, or current service contract. •
BSS DataVault Backup Support	• The DataVault is fully monitored and managed by BSS' Network Operations Center. Monitoring is performed for the DataVault device and local backup success or failure. • Daily verification tests are performed to verify the integrity of the data. • Each month, a manual recovery verification is performed. • Restoration of files and file folders is performed based on automated and BSS-created tickets. Service is included for Clients with fully Managed Packages. If a Client with the Basic Managed Service Package requests restoration, they will be billed using the hourly rate. • Preventive maintenance and management of imaging software is performed. • Firmware and software updates of the DataVault unit are included. • All problem analysis and resolution will be performed by the network operations team. • Troubleshooting and remediation of failed backup disks or other hardware issues is included. • See additional details in the BSS DataVault Services section under Additional Terms below.
BSS DataVault Backup Solution Offsite Storage	• Data is transferred offsite daily for additional protection in case of a catastrophe. • Secure remote (off-site) backup storage provided at a hardened Data Center ("DataVault Cloud"). • Data is encrypted with 256-bit AES encryption in transit. • Offsite backups are encrypted and stored in a SOC 2 compliant data centers. • All offsite backup data transfers are monitored for success or failure. • Troubleshooting and remediation of failed offsite backup data transfer is included. • DataVault Cloud server environments are available in the event of a disaster recovery scenario. • Data will be retained at remote storage for at least one year unless otherwise determined by BSS and Client. • See additional details in the BSS DataVault Services section under Additional Terms below.
Windows Computer Backup	• Back up an image of the computer directly to a secure data center in the cloud. • Scan for changes over an Internet connect and continuously back up files and folders. • Retain version history for up to 180 days. • Restore individual files or an entire computer image. • Limit of 1TB per Windows computer or laptop.
Switch Management & Support	• These must have vendor support. • Update firmware as needed. • Maintain VLANs and settings.
Wireless Access Points Management & Support	• These must have vendor support. • Update firmware as needed. • Maintain SSIDs and security settings.
Switch and Wireless Access Point Cloud Management Portal	• This may include a physical device, tied with an authorized cloud key, that allows for enterprise management of switches and wireless access points. • The administrative cloud portal provides a secure and centralized way to update firmware, apply configurations and security settings to network devices. • Statistics and tickets are automatically reported as needed.

Line of Business Application Support	• Current service contracts for each line of business application are required. • Provide commercially reasonable effort support for patches, updates, and other technical issues. • Client will rely on vendors or other third parties for support, application usage/workflow, training, bug fixes, extensive updates and patches, and any report writing or other functions that are beyond BSS's current skill sets or responsibilities as defined by BSS.
Printer and MFP Copier Support	• Provide network support and vendor management for business-class printers, plotters, and MFP/copiers ("Printers"). • All Printers must have the capability to attach to the network via network cable (Cat5 or better) and have current and supported operating systems. • MFP/copiers must have vendor support contracts. • Personal printers, which are typically ink jet printers, are not supported.
Miscellaneous Peripherals Support	• Support for devices such as time clocks, scanners, credit card machines, UPS devices, cameras, and similar items. • The devices listed above must have vendor support.
Microsoft 365 Environment Support	• Add, remove, and modify users in Microsoft 365 and Azure Active Directory. • Manage security groups, distribution groups, and device groups. • Manage Intune configuration profiles, compliance, multi-factor authentication, and conditional access. • Setup OneDrive folder redirection, password policy management, user training on best practices. • Manage Windows BitLocker encryption policies. • Manage SharePoint document libraries and associated permissions for existing sites that meet BSS approved standards. (New SharePoint document sites, subsites, and libraries are considered Projects and will be scoped and quoted) • Services are billable for Clients who do not have fully managed Service packages.
Vendor Management	• Current service contracts for each third-party vendor are required. • Contacting Client's third-party vendors such as Internet Service Providers, multi-function printer providers, and wiring/cabling providers for technical support. • Monitor the renewal of Internet domains. • Client authorizes BSS to contact third-party vendors and make changes on behalf of Client. • Client will provide BSS with a list of all third-party hardware and software vendors including accounting system, main line of business applications, other business software used, digital copiers, other IP-based peripherals, and any other IP-based equipment or software. • Any additions to third-party venders not listed at the signing of the Agreement, if acceptable to BSS, may result in an adjustment to the Client's monthly charges.
Mobile Device Management	• Includes support for Android tablets and iOS tablets only. Microsoft Surface computers or cell phones are not covered in this service. • Provide best effort support for setup by creating a client-specific sign on for the device if applicable, installing the Outlook application, and configuring email. • Requires mobile device management (MDM) licenses or Microsoft Intune for additional management. • For those devices under a mobile device management license, BSS will have the authority to set and enforce standards, reset phones to factory defaults should the need arise, and other activities required to provide control, support, and security. • There may be cases where the user will be directed to the phone vendor or phone service provider for support. Excluded services include cloud backups and restores to retain personal or non-Client specific business information.
Managed Antivirus for Macs	• Implement and manage an antivirus program on supported Mac operating systems and consolidates reporting and remediation. • Provides protection against and removal of viruses, malware, and potentially unwanted programs from managed devices through automatic and manual means. • Antivirus critical alerts create automatic support ticketing, and technical workflow for remediation. • Antivirus upgrades and updates are included and applied regularly. • Quarantined items are managed and removed as needed.

Technology Business Reviews	Regular meetings will be scheduled with Client's primary and/or key contracts. Meeting frequency and method will be determined by BSS and Client. Meetings may include topics such as the following: • Service delivery and reporting. • IT budgeting forecast. • IT strategic planning. • Proactive recommendations on technology requirements and direction. • Attend meetings as the technical liaison between Client and vendor. • Security and other pertinent educational discussions. • Relationship expectations.
Co-managed Tools	• Client may be given access to co-managed tools as described on the Quote. • May provide a separate ticket board for IT admin(s) typically in a co-managed agreement. • Licensed per admin user.
Tech Rider Computer Replacement Devices & Labor	• Computer/laptop hardware will be replaced according to the schedule described in the Quote for Pro Security and Securelink Cloud service plans. • Setup and installation are included. • Computers can include shared/equipment computers, desktops, laptops, custom computers for CAD or video, and Macs • Plans will be evaluated yearly and reviewed with Client. • See additional details in the Computer Replacement Plan section under Additional Terms below.
2-HARDWARE as a SERVICE (HaaS) MAY INCLUDE:	
HaaS BSS Firewall Solution	• Provide BSS-owned (HaaS) firewall and licensing at Client site to protect against hackers accessing the internal network(s) from outside the network(s). • Install, configure, and maintain network connectivity to only allow valid incoming traffic. • Perform firmware, security, and other updates as needed. • Administer firewall when changes are required for new applications or functions. • Setup VPN access according to best practice standards. • Periodic replacement of HaaS Equipment as needed. See additional details in the HaaS Equipment section under Additional Terms below
HaaS BSS Firewall Licensing	• Every Firewall device requires current and active licensing. • BSS-owned (HaaS) firewall licensing will be renewed as required to maintain active status. See additional details in the HaaS Equipment section under Additional Terms below.
HaaS BSS DataVault Backup Device or NAS	• Provide BSS-owned (HaaS) DataVault ("DataVault") device for provide backup and disaster recovery. • The DataVault device will either be a BDR (Backup Disaster Recovery) device or a NAS (Network Attached Storage) device. • The on-site DataVault unit acts as a local storage device (NAS and BDR) and stand-by server (BDR) in the event of an on-premises server failure. • Incremental backups are performed on the DataVault, initially set to every 1 hour between 7am and 6pm. • Data is encrypted with 256-bit AES encryption on the local DataVault storage. • Data will be retained on the local device for 60 days. • Install, configure, and maintain network connectivity and configurations. • Perform firmware, security, and other updates as needed. • Troubleshooting and remediation of failed backup disks or other hardware issues is included. • Periodic replacement of HaaS Equipment as needed. See additional details in the HaaS Equipment section under Additional Terms below

3-USER/COMPUTER SUPPORT MAY INCLUDE:	
User & Computer Support Requests	• Technical resources will be assigned as available and with the appropriate experience level required to resolve the issue. If necessary, other resources will assist or the ticket will be escalated to an alternative resource. • Support requests are included in fully managed packages. Basic support may be billed at an hourly rate.
Users - Email Only Support	• For those users with email requirements only where no support is required, licenses are provided, and the email application is set up. • Email-only users are not charged a per-user fee. • These users will not log into supported computers or BSS devices. • It is expected that email only users will not submit any support requests unless the request is specifically related to email issues on their mobile devices.
Best Practice Instructions	• Each user will be subscribed to BSS best practice instructions and email security tips which will be sent out on a regular basis. • Users may unsubscribe to be taken off this list.
Endpoint Managed Detection and Response (EDR)	• Manages the Windows Defender antivirus program on supported operating systems and consolidates reporting and remediation. • Implement to protect against and remove viruses, malware, and potentially unwanted programs from managed devices through automatic and manual means. • Antivirus critical alerts are integrated with the BSS MDR solution, automatic support ticketing, and workflow. • Antivirus upgrades and updates are included and applied regularly. • Quarantined items are managed and removed as needed. • Deploy and manage canaries to notify of potential malware and ransomware infections and shut down the device before the payload spreads. • Third-party 24/7 SOC monitoring and assistance in emergency response. • Review external port scans and remediate unnecessary open ports in network equipment and verify validity of undocumented devices.
Remote Monitoring & Management	• Install software agents on Covered Equipment. • Create an asset list of all personal computers. • Monitor for failures and hardware/software issues. • Basic routine system maintenance and optimization are performed. • Perform updates and patching.
Web & Content Filtering	• Configure devices to use trusted DNS sources that add additional protection from malware, botnets, ransomware, and phishing schemes. • Setup content filtering with block or allow access to many content categories by network, group, user, device, or IP address. • Whitelist and blacklist domains. • Provide reports as requested on cloud services used as well as trends.
Managed Antivirus Using Windows Defender	• Implement and manage Windows Defender • Provides protection against and removal of viruses, malware, and potentially unwanted programs from managed devices through automatic and manual means. • Antivirus critical alerts create automatic support ticketing, and technical workflow for remediation. • Antivirus upgrades and updates are included and applied regularly. • Quarantined items are managed and removed as needed.
4-OPTIONAL: MICROSOFT CARE PACKAGE:	

Microsoft 365 Environment Backup	• Service backs up Client's Microsoft 365 environment including Exchange Online, Teams, SharePoint, and OneDrive for Business. • Backups are performed as a snapshot three times daily. • Restores are performed as needed on individual objects or entire accounts. • Licensed by mailbox, all mailboxes must be included. • Backups are encrypted. • Backups are retained for at least one year.
Managed Detection & Response (MDR) for Microsoft 365	• Continuous monitoring of Microsoft 365 cloud environment and applications, including SharePoint, Teams, Outlook, Word, Excel, and other Microsoft 365 online programs. • Generate tickets to document potential threats and notify help desk of suspicious activity. • Provide proactive automatic and manual remediation of suspicious activity, vulnerable accounts, anomaly detection, rules and forwarding, and privilege escalations. Remediation will be performed unless the requirements are deemed Out of Scope of this Services Agreement. • Deploy and manage canaries to notify of potential malware and ransomware infections and shut down the device before the payload spreads. • Third-party 24/7 SOC monitoring and assistance in emergency response.
5-OPTIONAL: USER CARE PACKAGE:	
Online Training Library	• Provides a self-service eLearning library for Microsoft 365 and other products. • Integrates with Microsoft Teams. • Incorporates full-text index searching.
Security Awareness Training	• Perform a baseline assessment to determine the phishing risk of the organization. • Provide simulated phishing emails to employees to continuously test email security knowledge. • Provide online training videos to further educate employees on email and cybersecurity.
6-OPTIONAL: SECURITY CARE PACKAGE:	
Dark Web Email/Password Compromise Monitoring	• The dark web is monitored through a third-party application for Client user credentials that have been compromised. • When a compromise is found, a ticket is created, and the user is notified and presented with steps to take to avoid risk. • The dark web monitoring services utilize the resources of third-party solution providers. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, BSS does not guarantee that the dark web monitoring service will detect all actual or potential uses of Client's designated credentials or information.
Enterprise Desktop MFA Management	• Enterprise level multi-factor authentication (MFA) software to provide secondary authentication for network, computer, and application credentials. • Implement MFA on email, laptops, desktops, supported line-of-business applications, and other devices/applications as available by vendor. • Provide support for changes and remediation for compromised accounts.
Hard Drive Encryption Management	• Secure hard drives on Windows laptops and desktops with BitLocker encryption. • Encryption keys are securely documented.
Security Information and Event Management (SIEM)	Provide an agent and third-party service to perform the following: • Aggregate data from logs and events from various security, network, and computer devices. • Explore aggregated data to discover details of a security incident or potential security incident. • Store long-term historical data for compliance and forensic investigations.

OTHER PRODUCTS AND SERVICES MAY INCLUDE:	
VoIP Phone Support	• Provides installation and support of VoIP phone systems, including physical phone models that are supported by BSS suppliers with current VoIP capabilities. • BSS supports only VoIP system BSS implements • BSS will work with other third-party provided VoIP systems. • BSS does not support traditional phone systems.

Additional Description of Services

The following additional details further explain and define the scope of the Services.

Covered Equipment; Environment

The Services will be applied to the equipment, hardware, software, and users (collectively, the "Environment" or "Covered Services") listed in the Quote. If there are additional items not listed on the Quote that are to be included in "Covered Equipment" a "Managed Environment Schedule" will be included as an addendum to the Services Statement. Items that are not included in the Environment will not receive or benefit from the Services.

Physical Locations Covered by Services

Services will be provided remotely unless, in BSS' discretion, BSS determines that an onsite visit is required. Onsite visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless BSS agrees otherwise, all onsite Services will be provided at Client's primary office location listed in the Quote. Client will provide to BSS a list of all the addresses of Client locations during onboarding. Trip charges or additional fees may apply for onsite visits if outside the metropolitan area of the BSS offices. Please review the Service Level section below for more details.

Term; Termination

The Services will commence on the Commencement Date and will continue through the initial term listed in the Quote ("Initial Term"). Onboarding may not be completed within a 30-day period.

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

1. Client may not cancel the Agreement until the end of the first year from the Commencement Date. On the one-year anniversary of the Commencement Date, Client may terminate the Agreement with 60 days' notice.
    i. All HaaS equipment provided to the Client requires payment for remaining term (up to 36 months) of the original agreement. The 60-day Agreement cancellation does not apply to the HaaS section of the Agreement.
    ii. The BSS DataVault Backup Solution Offsite Storage requires payment for the remaining term (up to 36 months).
2. BSS may terminate the Agreement with 60 days' notice for any reason.
3. Client must pay all amounts owed including late fees prior to BSS providing any administrative passwords. Once the administrative passwords have been provided to Client or Client's new designated provider, BSS will no longer provide support even though the termination date has not yet passed.
4. Termination Terms:
    i. There will be no termination fees owed to BSS other than an off-boarding fee equal to the last month's Agreement invoice.
    ii. If BSS terminates the Agreement, there will be no off-boarding fee.

iii. Replacing firewall, backup, antivirus, spam filter, and other BSS supplied hardware or tools are the responsibility of the Client prior to the termination end date.

iv. BSS will assist Client in the orderly termination of services, including timely transfer of the services to another designated provider. Client agrees to pay BSS the actual costs of rendering such assistance.

5. Reference additional terms in the MSA section "Term; Termination."

Auto-Renewal. After the expiration of the initial Service Term, the Service Term will automatically renew for twelve (12) months unless either party notifies the other of its intention to not renew the Services no less than thirty (30) days before the end of the then-current Service Term.

Microsoft NCE Licensing. Regardless of the reason for the termination of the Services, you will be required to pay for all NCE Licenses that BSS acquires on your behalf. Please see "Microsoft Licensing Fees" in the Fees section below for more details.

Assumptions/Minimum Requirements/Exclusions

- The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements. **A surcharge may be added if items do not meet these requirements.**
- **All desktops and laptops** (Windows or Mac), tablets, and servers must be included on the support plan.
- Server hardware must be under current warranty coverage and less than six years old.
- Workstations, personal computers, and laptops must be less than six years old.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed and vendor supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The Environment must have the BSS DataVault Offsite Backup Solution & Support for any on-premise servers and the BSS Microsoft 365 Environment Backup for Microsoft cloud-based services.
- All wireless data traffic in the environment must be securely encrypted.
- There must be a Broadband or better Internet connection with an outside static IP address assigned to a network device, allowing VPN/RDP control access.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups, or the data stored on the backup devices. BSS does not guarantee the integrity of the backups, or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Statement.
- Client must provide BSS with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by BSS.

Exclusions. Services that are not expressly described in the Quote will be Out of Scope and will not be provided to Client unless otherwise agreed, in writing, by BSS. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by BSS in writing:

- Customization of third-party applications or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Hardware that is over six years old.
- Data/voice wiring or cabling services of any kind.
- UPS batteries.
- Equipment relocation.
- The cost to bring the Environment up to the Minimum Requirements.

- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.
- The cost of any software, licensing, or software renewal or upgrade fees of any kind.
- The cost of any third-party vendor or manufacturer support or incident fees of any kind.
- Website creation or maintenance.
- Phone systems not installed by BSS.
- Failure due to acts of God, building modifications, power failures, or other adverse environmental conditions or factors.

Service Levels

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis; response, repair, and/or remediation services (as applicable) will be provided only during business hours unless otherwise specifically stated in the Quote. BSS will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by BSS in BSS' discretion after consulting with the Client. All remediation services will initially be attempted remotely; BSS will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Trouble/Severity	Priority	Basic Protection	Pro Security	Securelink Cloud	Resolution Time
Critical: Business is unable to continue (e.g., all users and functions unavailable)	1	4 hours	1 hour	1 hour	ASAP - Best Effort
Significant Degradation: Key systems are unavailable (e.g., large number of users or business critical functions affected)	2	6 hours	2 hours	2 hours	ASAP – Best Effort
Limited degradation of service: Limited system functionality (e.g., some users or functions affected)	3	Next Business Day	4 hours	4 hours	ASAP - Best Effort
Small service degradation or irritation: Business process can continue (e.g., one user affected, or can schedule onsite visit)	4 & 5	As Available	8 hours	8 hours	ASAP - Best Effort

* All time frames are calculated as of the time that BSS is notified of the applicable issue/problem by Client through BSS' designated support portal, help desk, or by phone at the support numbers listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts. Help desk support provided outside of BSS normal support hours will be billed to Client at the hourly rates described in the SOW.

Fees; Payment

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

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

Increases. In addition, BSS reserves the right to increase BSS monthly recurring and data recovery fees no more than once per year as stated in the Quote. As stated in the MSA, Third-Party Service costs will be passed through to you as they occur with as much advance notice as reasonably possible. Your continued acceptance or use of the Services will indicate your acceptance of the increased fees.

Travel Time. If onsite services are provided, BSS will travel to your offices within the metropolitan area of BSS offices at no charge. Time spent traveling beyond the metropolitan area (*e.g.,* locations that are beyond the metropolitan area of BSS offices or occasions on which traffic or weather conditions extend BSS drive time) will be billed to you at BSS then current hourly rates or

will incur a site charge. In addition, you will be billed for all tolls, parking fees, and related expenses that BSS incurs if BSS provides onsite services to you.

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

Monthly Invoicing: Monthly fees after the Commencement Date payment will be invoiced on or about the first of the month. If the Commencement Date starts during a partial month, the invoice may be prorated. Payment is due within 15 days of the invoice date.

Automated Payment. You may pay your invoices by credit card and/or by ACH, as described below. If you authorize payment by credit card and ACH, then the ACH payment method will be attempted first. If that attempt fails for any reason, then BSS will process payment using your designated credit card.

- **ACH**. When enrolled in an ACH payment processing method, you authorize BSS to electronically debit your designated checking or savings account, as defined and configured by you in BSS' payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. BSS will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.
- **Credit Card**. When enrolled in a credit card payment processing method, you authorize BSS to charge your credit card, as designated by you in BSS' payment portal, for any payments due under the Quote. There will be a three (3) percent charge for payment by credit card.

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

Out of Scope Work. Out of Scope work requires a Quote and will be billed as stated in the Quote SOW. Out of Scope work is defined as BSS support activities which are Not included by BSS as part of BSS' monthly agreement. Any time that is spent by BSS resolving an issue that is Out of Scope is billed at an hourly rate in addition to the monthly agreement.

Projects. Projects require Client preapproval through accepting a separate Quote and will be billed at the rate stated on the project Quote. Projects are defined as new installs, upgrades, or additions to the current Environment. Improvements that take Out-of-Scope items and put them in a state that is In Scope, or major changes to the functionality of the services are considered projects. Project work will typically require greater than one hour to complete or will require more than one resource.

Additional Terms

Authenticity

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If BSS asks for proof of authenticity and/or licensing, you must provide BSS with such proof. All minimum hardware or software requirements as

indicated in a Quote or this Services Statement ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of BSS providing the Services to you.

Remediation

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

Configuration of Third-party Services

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

Modification of Environment

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

Co-Managed Environment

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by BSS), BSS will endeavor to implement the Services an efficient and effective manner; however, (a) BSS will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from BSS' position on a Service-related matter, BSS will yield to the Co-Managed Provider's determination and bring that situation to your attention.

Antivirus/Anti-malware

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

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under BSS' then-current hourly labor rates. Given the varied number of possible Security Incidents, BSS cannot and does not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data impacted by the incident will be recoverable. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible

disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the Environment, or (ii) prevents normal access to the Environment, or impedes or disrupts the normal functions of the Environment.

Environmental Factors

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

Fair Usage Policy

BSS' Fair Usage Policy ("FUP") applies to all Services that are described or designated as "unlimited." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during BSS' normal business hours only and are subject to BSS technicians' availabilities, which cannot always be guaranteed. In addition, BSS reserves the right to assign BSS technicians as BSS deems necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with BSS' ability to provide BSS' services to BSS' other customers.

Hosted Email

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

BSS DataVault Services

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

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

Excluded Services. The following services are excluded:

1. The DataVault hardware replacement cost and the cost associated with hardware replacement due to damage, theft or destruction.
2. Backing up of local data that may reside on desktop and laptop machines.
3. Any of the Microsoft 365 products such as email, SharePoint, OneDrive, etc.

Ownership of the Data. The following describes ownership of the data:

1. The backup data being stored on the DataVault and at the Data Center remains the sole property of the Client. If the Client chooses to terminate services, BSS will assist Client in the orderly termination of services. This could involve copying the backup image to an external drive which can be synchronized with the data on the DataVault. The Client agrees to pay BSS the actual costs of rendering such assistance.
2. Client acknowledges and releases BSS from any liability of programs or data on the BSS DataVault, which may be lost while the BSS representative is performing the services, as well as any consequential losses that may result. The client further releases BSS from all responsibility for the recovery and/or reentry of said information from the BSS DataVault.

Facilities. The Client agrees that BSS may gain access to certain Client facilities. Facilities must maintain proper cooling and humidity controls as to not adversely affect hardware. Facility access may be denied for any reason at any time, however if access to facilities is denied, The Client understands that BSS may be unable to perform their duties adequately and if such a situation should exist, BSS will be held harmless.

Passwords. BSS acknowledges that it must have access to any and all systems and resources to perform their duties under this agreement. As such, it must have access to any and all server passwords. Bear in mind that the backup data will always be encrypted and not accessible to anyone who does not have the password. If the encryption password is lost, the backup data will be inaccessible.

Warranty. The following describes the warranty:

1. BSS warrants that the work will be performed to the best of its ability and in accordance with reasonable and customary practices prevailing at the time for its business.
2. The DataVault units cannot be modified in any way or the warranty and the management agreements are voided. This includes adding software applications to the DataVault itself, adding memory or hard drives.
3. No other warranties exist, expressed or implied.

Supported Technologies. Windows Servers that are Mainstream or are in Extended Support from Microsoft.

Procurement

Equipment and software procured by BSS on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, BSS does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third-party return policies and/or re-stocking fees, all of which shall be Client's responsibility in the event that a return of the Procured Equipment is requested. BSS is not a warranty service or repair center. BSS will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which BSS will be held harmless, and (ii) BSS is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Sample Policies, Procedures

From time to time, BSS may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. BSS

does not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

Penetration Testing; Vulnerability Assessment

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

No Third-Party Scanning

Unless BSS authorizes such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request BSS (and BSS elects) to perform those services, those services will be billed to you at BSS' then-current hourly rates.

HaaS Equipment

BSS will provide you with the HaaS Equipment described in the Quote or, if no hardware is expressly designated as HaaS Equipment in the Quote, then a complete list of HaaS Equipment be provided to you will under a Managed Environment Schedule addendum.

Internal Use Only. You will use all BSS-hosted or BSS-supplied equipment and hardware (collectively, "Infrastructure") for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the Infrastructure available to any third party without BSS' prior written consent. You agree to refrain from using the Infrastructure in a manner that unreasonably or materially interferes with BSS' other hosted equipment or hardware, or in a manner that disrupts or that is likely to disrupt the services that BSS provides to BSS' other clientele. BSS reserves the right to throttle or suspend your access and/or use of the Infrastructure if BSS believes, in BSS' sole but reasonable judgment, that your use of the Infrastructure is violates the terms of the Quote, this Services Statement, or the Agreement.

Ownership of HaaS Equipment. You agree that ownership of the Equipment shall not be transferred to you. You agree and understand that equipment is to be maintained completely by BSS. You will not attempt to sell, resell, tamper with, troubleshoot, repair, move, add, etc. to this Equipment without written permission of BSS, and BSS shall be entitled to immediately terminate this Agreement should there be any tampering, repair attempt or service completed by another party on the HaaS Equipment.

Additional Loss Payee. You agree to make its best efforts to keep equipment safe, secure and protected while in its possession. You agree to keep current insurance on HaaS Equipment while in its possession and list BSS as an additional loss payee, and, upon request, Client will provide proof that BSS is listed as an additional loss payee, providing a current copy of its insurance declaration sheet showing BSS or its designated third-party as a loss payee. You also further agree to be responsible for any and all costs for the repair or replacement of Equipment while in your possession should it be damaged or repaired by an unauthorized third party.

Periodic Replacement of HaaS Equipment. From time to time and in BSS' discretion, BSS may decide to swap out older HaaS Equipment for updated or newer equipment. (Generally, equipment that is five years old or older may be appropriate for replacement). If BSS elects to swap out HaaS Equipment due to normal, periodic replacement, then BSS will notify you of the situation and arrange a mutually convenient time for such activity.

Return of HaaS Equipment. Unless BSS expressly directs you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that BSS installed in the HaaS Equipment. Doing so could result in network vulnerabilities and/or the

continuation of license fees for the software agents for which you will be responsible, and/or the requirement that BSS remediate the situation at BSS' then-current hourly rates, for which you will also be responsible. Within ten (10) days after the termination of HaaS-related Services, Client will provide BSS access to the premises at which the HaaS Equipment is located so that all such equipment may be retrieved and removed by BSS. If you fail to provide BSS with timely access to the HaaS Equipment or if the equipment is returned to BSS damaged (normal wear and tear excepted), then BSS will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Obsolescence

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

Proper Use of Systems

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

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

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

Licenses

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

Computer Replacement Plan

The Computer Replacement Plan system includes computer, monitor (only if needed), mouse, keyboard, Microsoft Operating System and does not include applications. If desired, Client may choose to upgrade certain hardware and software components through BSS at the time of the system replacement, such as Adobe Acrobat, more RAM, bigger CPU, better video, etc. The basic specifications will always meet or exceed the recommended specifications, as published by Microsoft, for the current release of desktop Operating System and the system being replaced.

Client will work with their BSS Account Manager to select the equipment specifications each year. Models and pricing may change due to availability and/or supersession of new SKUs and BSS at its sole discretion may substitute appropriate models.

Hardware warranties are handled via the equipment manufacturer's warranty policy.

Additional units to the SOW will require an installation fee for labor and will be quoted as a project with a discounted fee. These additional units will not be part of the Tech Computer Replacement Plan until the annual review of the Computer Replacement Plan Equipment List where the costs, number of computers, and or computer specifications may change based on agreement between BSS and Client.

BSS will take possession of and dispose of the old system being replaced after performing a security erase of all data on that system. If the client wishes to keep old unit, BSS will remove BSS' software and make it "home ready" for the fee specified on the Quote.

Sales Tax. Upgrades and Add-ons and other hardware/software purchases will have Sales Tax added.

Tax Benefits. Client shall be entitled to such deductions, credits, and other tax benefits as are provided by federal, state, and local income tax law to an owner of the Computer Replacement Plan computers.

Personal Property Taxes. Client will be responsible for filing all personal property tax returns and paying all personal property taxes for items covered by this agreement.