Services Guide

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

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

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

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

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

Initial Audit / Diagnostic Services

Before managed services begin, we will perform an initial audit and onboarding assessment of your existing technology environment to help us understand the condition, configuration, security posture, supportability, and business risks associated with your systems.

This Initial Audit may include, as applicable, a review of your network, servers, workstations, cloud services, Microsoft 365 (or if applicable, Google Workspace) environment, backup systems, security tools, remote access methods, endpoint protection, firewall configuration, wireless environment, administrative accounts, licensing, line-of-business applications, password maintenance processes, and other technology assets that we reasonably determine may be relevant to the managed services.

The Initial Audit is not a guarantee that all issues, deficiencies, security risks, vulnerabilities, unsupported systems, licensing issues, data loss risks, compliance gaps, or other issues will be discovered. Some issues may be hidden, intermittent, or only discoverable after services begin ("Latent Issues"). Latent Issues discovered after managed services begin may require additional resources, fees, or remediation for which we will not be responsible unless we expressly agree otherwise in writing. You understand and agree that unless we expressly state otherwise in a Quote, we will not be responsible or liable for problems or errors related to Latent Issues.

Depending on the results of the Initial Audit, we may determine that certain systems, devices, applications, configurations, or environments are not supportable in their current condition ("Current Issues"). Under those circumstances, you will be required to approve reasonable replacement, upgrades, documentation, security changes, or other corrective measures before we assume responsibility for supporting those items. If you decline or delay recommended remediation of Current Issues, we will not be responsible or liable for resulting service issues, downtime, security incidents, data loss, compliance failures, performance problems, or other consequences arising from the uncorrected condition(s). If your delay or declination renders it reasonably impracticable for us to implement our managed services, we may terminate the applicable Quote by providing you with three (3) business days' notice.

The Initial Audit requires your cooperation and input. This means that we may require you to provide us with passwords, administrative credentials, licensing information, existing contracts/documentation (all of which will be considered to be your Confidential Information), as well as access to your company's stakeholders before the Initial Audit can be completed.

Onboarding Services

Onboarding is the stage during which we prepare the managed environment ("Environment") for the managed services described in the Quote. During this phase, we deploy required tools and will work with your Authorized Contact(s) to review the information we need to prepare the Environment to receive the managed services.

It is your responsibility to have your previous IT service providers' tools and software agents ("Prior Tools") removed in cooperation with our installation of our tools, as well as to uninstall then-existing administrative passwords or keys (or provide us with those passwords and keys) as necessary for us to implement our services. Additional charges may apply if we are required to uninstall Prior Tools, seize administrative access, or undertake any other efforts reasonably necessary for us to acquire administrative access.

Please note: If we are unable to uninstall or disable Prior Tools remotely, then an onsite visit may be required for which additional fees, such as travel time, may apply. In any event, if Prior Tools cannot be removed then we will bring that situation to your attention and, to the extent reasonably practicable, quarantine the Prior Tools so they become inoperative. We do not warrant or guarantee that all Prior Tools will be capable of being removed permanently, or that unremovable Prior Tools will become or remain inoperative.

Onboarding generally occurs in stages as follows:

- Discovery/Information Gathering: We collect information needed to more thoroughly understand your business, your technology environment, your users, and your current risks. The more complete and accurate this information is, the faster and more effectively we can onboard your environment.

- Access, Credential and Admin Control: During this stage, we establish secure administrative access to the systems within the agreed scope of services. Delays in providing access may delay onboarding and may limit our ability to identify or correct issues.

- Tool Deployment: We deploy the tools required to monitor, manage, secure, and support the Environment. These tools allow us to perform the services described in Quote and as described in this Guide.

- User, Support, and Communication Setup: We establish the communication and support procedures that will apply once the Services go live. This includes creating ticket submission methods and expectations for emergency and non-emergency requests.

- Documentation: We document the Environment so that our support is not dependent on memory or a single individual's knowledge. Proper documentation helps us respond faster, reduce errors, and provide more consistent service.

If Latent Issues are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. **Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of Latent Issues.**

The duration of the onboarding process depends on many factors, some of which may be outside of our control, such as product availability/shortages, required third-party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

Ongoing / Recurring Managed Services

The table below describes all managed services provided or facilitated by ICS; however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). **Please review the Quote to determine which of the managed services listed below will be provided to / facilitated for you.**

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

Managed Services

(Please refer to the Quote to determine which Managed Services you will be receiving.)

SERVICES	GENERAL DESCRIPTION

Asset Administration	This service consists of the tracking, documentation, and administrative management of Client's IT assets throughout their lifecycle. Through this service, Client can maintain better visibility into its technology environment which supports planning and budgeting, and promotes more efficient deployment, support, maintenance, and retirement of covered assets.
	
	Included in the service are the following:
	• Device lifecycle management (hardware replacement planning, OS lifecycle tracking, and warranty management; reviewed quarterly in Business Technology Review)
	• Microsoft 365 Tenant Management (user administration, licensing, security policies, conditional access, MFA enforcement and configuration management, Exchange / SharePoint / Teams admin)
	• Licensing Management (Microsoft and MSP-provided services) including provisioning, deprovisioning, and optimization
	• New hire onboarding (*e.g.,* device setup, Microsoft 365 provisioning, security configuration)
	• Termination / offboarding (*e.g.,* account disablement, access revocation, data retention handling)
	• Supported Software subscription expiration tracking
	• Domain name expiration tracking (Client must supply us with a list of all URLs to be tracked)
	• Hardware and software purchase specification
	• Maintain network documentation and secure password storage
	• Act as liaison (if required) with hardware and software vendors and service providers for Managed Hardware and Supported Software
	• Proactive maintenance and routine additions, deletions or changes to the following:
	  ○ Security groups
	  ○ Settings
	  ○ Configurations
	  ○ Policies
	
	Third-party licensing (e.g., Adobe and other external vendors) is supported on a best-effort basis; Client retains ownership and responsibility for licensing and billing.
	
	Please note: Asset Administration services are administrative in nature and do not, by themselves, include procurement, physical inventory verification, repair, replacement, disposal, onsite inspections, warranty enforcement, or auditing of asset accuracy unless

	expressly stated in the applicable Quote. Asset records maintained by ICS are based on information available from Client, distributors, vendors, software tools, and network discovery utilities, and therefore may not always reflect real-time or complete information.
Application Whitelisting	This service helps reduce malware, ransomware, and unauthorized software by limiting which applications are permitted to run in Customer's managed environment. Rather than relying solely on detection after execution, application whitelisting enforces a "default deny" posture so that only approved applications, scripts, and installers are allowed to execute based on defined rules and policies. As part of this service, we will: • Assess the environment and establish a baseline of commonly used applications and required business software. • Implement and manage allow/deny policies based on application identity (publisher/signature, file hash, path, certificate, or application name), as supported by the selected technology. • Create approval workflows for new software requests, including review of business justification and security risk. • Deploy policies to in-scope endpoints/servers and tune policies over time to reduce false blocks while maintaining security objectives. • Monitor and report on blocked execution events, policy violations, and trends (e.g., repeated attempts to run unauthorized tools). • Maintain exceptions for approved use cases (e.g., line-of-business apps, signed administrative tools, approved scripting), subject to documented approval. **Important**: Application whitelisting is a risk-reduction control. It may block legitimate applications until they are approved and added to the allow list. To that end, Customer must work with us to create an accurate list of required business applications, including line-of-business software, plugins, and any specialized tools needed by Customer's users. Customer must also notify us of any mission-critical systems, workflows, and time-sensitive operational requirements so whitelisting policies can be designed with appropriate safeguards. Customer should anticipate an initial tuning period after deployment. **Note**: By using this service, Customer acknowledges that: • Some applications may be blocked until approved and allow-listed. • Emergency or highly customized software may require additional review time and may not be compatible with strict whitelisting controls. • Systems or devices excluded from scope (or devices not consistently connected/managed) may not receive current policies, reducing effectiveness.
Backup and File Recovery	Backup services may be delivered to endpoints, servers, or network attached storage devices. Please refer to the Quote to determine which devices will receive backup services. **Do not assume that all devices connected to or included in the managed network will receive backup services. Only those devices specifically stated in the Quote will receive these services.** This service includes the implementation and facilitation of a backup and file recovery solution from our designated Third-Party Provider. • 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance"). • Troubleshooting and remediation of failed backup disks. • Preventive maintenance and management of imaging software. • Firmware and software updates of backup appliance. • Problem analysis by the network operations team.

	• Monitoring of backup successes and failures. • Daily recovery verification. Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities. Backup Retention: Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Quote. This includes both on-premise and cloud backups. • *On-Premise Backups* All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis. • *Cloud Backups* All cloud backups will be stored in a secure, off-site location that meets the organization's security standards. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis. Backup Alerts: Managed servers will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: info@chooseics.com ○ Web portal: ICS Support | ICS, Inc. ○ Telephone: 256-760-8239 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data.
Backup Monitoring	Implementation and facilitation of a backup monitoring solution from our designated Third-Party Provider. Features include: • Monitoring backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helping ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications. **Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.**
Breach Remediation	Our breach remediation service endeavors to restore and stabilize the customer's IT environment following a confirmed or suspected security incident, using the services and tools to which the customer is actively subscribed. Depending on the circumstances of the breach, this service may include: • Environment Stabilization: Contain and mitigate the impact of the incident within the managed environment, including isolating affected systems, disabling compromised accounts, and removing identified threats using deployed security tools.

	• Service-Level Remediation: Investigate and remediate activities performed through our standard toolset (*e.g.*, endpoint protection, monitoring and management tools, email security platforms) to the extent such tools are part of the customer's subscribed services. • Backup Restoration: Restoration of data and systems from available backups, subject to backup scope, retention limits, and data integrity at the time of the incident. • System Recovery Assistance: Rebuilding or reconfiguring affected systems using standard configurations, where applicable. Exclusions and Limitations: This service does not include: ○ digital forensics, root cause analysis, or formal incident investigations; ○ engagement of third-party forensic firms, legal counsel, public relations firms, or other external specialists; ○ recovery of data not contained within the MSP-managed backup systems; ○ remediation of systems, applications, or environments not covered under the customer's active service agreement; ○ guarantees of full data recovery, system integrity, or prevention of future incidents. All services are performed on a commercially reasonable efforts basis and are subject to the limitations of the Customer's existing infrastructure, subscribed services, and the nature and severity of the incident.
Cloud Managed Detection & Response (MDR)	This service monitors Client's cloud-based systems, accounts, identities, applications, and related activity for signs of malicious, unauthorized, or suspicious behavior. The service is intended to identify potential threats affecting Client's cloud environment, investigate relevant alerts and events, and facilitate or recommend appropriate response actions. Please note: Cloud MDR improves visibility into cloud risks, but it does not eliminate all threats, guarantee that all malicious activity will be detected, or replace Client's obligation to maintain secure cloud configurations, access controls, and security policies.
Cybersecurity Assessment	Our Cybersecurity Assessment service is designed to provide a high-level evaluation of the security posture of the managed IT environment through targeted vulnerability scanning and gap analysis. This service includes the use of automated tools to identify known vulnerabilities, misconfigurations, and potential exposure points within systems, networks, and devices. In addition, we perform a comparative gap analysis to assess the alignment of the environment against generally accepted security practices and baseline standards. The assessment is intended to highlight areas where the environment may require remediation, enhancement, or additional safeguards. Deliverables may include a summary of identified vulnerabilities, risk categorizations, and recommended corrective actions. Please note: This service is diagnostic in nature and does not include remediation, continuous monitoring, penetration testing, or formal compliance audits unless separately agreed in a Quote. We do not guarantee that all vulnerabilities will be detected in the assessment phase.
Dark Web Monitoring	Implementation and facilitation of a Dark Web Monitoring solution from our designated Third-Party Provider. Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web. If compromised credentials are found, they are reported to Help Desk Services staff who will review the incident and notify affected end-users.

	Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.
Device Encryption (BitLocker Management)	Our Device Encryption / BitLocker Management service consists of the deployment, configuration, monitoring, and administrative management of encryption technologies designed to help protect data stored on covered devices from unauthorized access in the event of loss, theft, or improper physical access. For Microsoft-based environments, this includes the implementation and management of BitLocker (or other comparable device encryption tools) on compatible endpoints. This Service includes enabling encryption on supported devices, configuring encryption policies, escrowing and maintaining recovery keys where supported, monitoring encryption status, assisting with remediation of encryption-related alerts, and helping confirm that covered devices remain encrypted in accordance with the applicable service configuration. It also includes administrative assistance relating to encryption recovery events, such as providing access to recovery keys through approved procedures when a device is locked, requires recovery authentication, or experiences certain hardware or software changes that trigger a recovery event. Please Note: Device Encryption / BitLocker Management Services help reduce the risk of unauthorized access to data stored locally on encrypted devices, but they do not guarantee the prevention of data loss, unauthorized access, exfiltration, or misuse. Encryption services do not protect against compromises involving authorized credentials, malware operating under valid user access, cloud-stored data, improperly configured permissions, insecure third-party applications, or data transmitted outside of the encrypted device. In addition, encryption functionality may be limited by device compatibility, hardware condition, operating system edition, firmware configuration, TPM availability, user action, or other environmental factors.
Device Lifecycle Management	This service helps Client plan for, track, maintain, refresh, and retire managed technology devices throughout their useful life. This service may include assistance with device inventory review, lifecycle status tracking, warranty and support status review, replacement planning, refresh recommendations, procurement coordination, deployment coordination, configuration assistance, asset tagging, documentation updates, and retirement or disposal coordination. As part of this service, we may help identify devices that are aging, unsupported, underperforming, out of warranty, incompatible with current business or security requirements, or otherwise appropriate for replacement, upgrade, or retirement. We may also provide recommendations regarding standardization, device refresh timing, operating system compatibility, vendor support status, and general business or technical suitability. Please note: Unless expressly stated in an applicable Quote, this service does not include the cost of hardware, software, licenses, subscriptions, training or other project-based services. If you request that we dispose of outdated or obsolete equipment, we may do so subject to additional fees and separate terms. (Please see E-Waste Disposal in the MSA for additional information). Client will remain responsible for approving purchases, disposal decisions, and any required downtime or impacted user availability.
Domain Name Server (DNS) Filtering	This service inspects DNS requests and blocks access to domains that are known to be malicious, suspicious, prohibited, or inconsistent with Client's acceptable use or security policies. The service includes malicious domain blocking, category-based filtering, custom allow/block lists, DNS-layer threat intelligence, policy enforcement by user, group, device, or location, and related logging, reporting, and alerting.

	The service is intended to reduce exposure to phishing, malware, ransomware, inappropriate content, and other unwanted internet destinations by interrupting access attempts at the DNS layer before a full connection is established. Please note: DNS Filtering helps block access to known or suspected harmful or unwanted domains, but it is not a complete security solution. It works at the DNS layer, which means it may not stop threats that bypass DNS, use trusted or compromised domains, connect by direct IP address, or otherwise avoid standard domain-based controls. Because of these limitations, DNS Filtering should be used as one layer of a broader security program and not as a substitute for other protective measures.
Email Threat Protection	Implementation and facilitation of a trusted email threat protection solution from our designated Third-Party Provider. • Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against "looks like" and "sounds like" versions of domain names. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.** **All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.**
Email Security Service – Domain Protection (DMARC Enforcement)	This service includes implementation and management of DMARC (Domain-based Message Authentication, Reporting & Conformance) to help protect your organization from email-based threats, including phishing, spoofing, and business email compromise. DMARC works in conjunction with industry-standard authentication protocols such as SPF and DKIM to verify that emails sent from your domain are legitimate and authorized. This service includes: • **DMARC Policy Configuration:** Establishment and enforcement of DMARC policies (monitoring, quarantine, or reject) to control how unauthorized emails are handled. • **Email Authentication Alignment:** Configuration and validation of SPF and DKIM records to ensure proper alignment with DMARC requirements. • **Threat Protection:** Reduction of domain spoofing, phishing attacks, and fraudulent email activity targeting your organization or its customers. • **Reporting & Visibility:** Ongoing monitoring and analysis of DMARC reports to identify unauthorized sending sources and improve email security posture. • **Policy Optimization:** Gradual enforcement strategy to minimize disruption to legitimate email while strengthening protection over time. For this service to work effectively, the customer must: • Maintain accurate records of authorized email sending services and notify us of any changes (*e.g.*, new marketing platforms, third-party senders); • Provide timely access to DNS management and email systems as required for configuration and updates; and • Review and approve enforcement changes (*e.g.*, moving from monitoring to reject policies).

	Please note: DMARC protects against domain spoofing, but it does not eliminate all phishing risks, particularly where attackers use lookalike domains. Effectiveness depends on proper configuration of SPF/DKIM and cooperation from third-party email service providers. Unless we indicate otherwise in a Quote, remediation of compromised accounts or internal threats is outside the scope unless separately contracted. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important additional details.**
Endpoint Detection & Response	Implementation and facilitation of an endpoint detection and response solution from our designated Third-Party Provider. • Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detection of unauthorized behaviors of users, applications, or network servers. • Blocking of suspicious actions before execution. • Analyzing suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices such as laptops, desktops, and servers. • Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more. • Whitelisting for legitimate scripts. • Blocking of unwanted web content. • Detection of advanced phishing attacks. • Detection / prevention of content from IP addresses with low reputation. *** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry-leading third-party solution provider. • Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats. Please note: Untrained staff could create or cause security vulnerabilities. Client must notify us if Client hires new staff/personnel, since those persons must undergo awareness training to ensure consistent security protocols and processes across Client's IT environment. In addition, Client's personnel may receive reminders, generally sent by email, reminding them to participate in the awareness training. It is Client's responsibility to ensure that its staff undertakes training on a consistent basis. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Extended Detection & Response (XDR)	Implementation and facilitation of an endpoint malware protection solution with extended functionalities from our designated Third-Party Provider. • Automated correlation of data across multiple security layers*—email, endpoint, server, cloud workload, and the managed network, enabling faster threat detection. • Provides extended malware sweeping, hunting, and investigation. • Allows whitelisting for legitimate scripts.

	• Next-generation deep learning malware detection, file scanning, and live protection for workstation operating system. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection. • Managed detection, root cause analysis, deep learning malware analysis, and live response. • On-demand endpoint isolation, advanced threat intelligence, and forensic data export. * Requires at least two layers (*e.g.*, endpoint, email, network, servers, and/or cloud workload.) **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Firewall as a Service (firewall appliance provided by ICS)	• Provide a firewall configured for your organization's specific bandwidth, remote access, and user needs. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality. • Firewall appliance is subject to "Hardware as a Service" terms and conditions located in this Guide. • Firewall appliance must be returned to ICS upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.
Firewall Solution (firewall appliance provided / purchased by Client)	• Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality. Please note: Client's firewall appliance must be compatible with the monitoring, management, security, automation, and support tools, agents, integrations, and related software utilized by us in connection with the Services. Client's firewall appliance must also permit required network traffic, agent communications, logging, alerting, update functions, and administrative access necessary for us or our designated solution provider(s) to perform the Services. If a firewall appliance is incompatible, unsupported, inaccessible, improperly configured, end-of-life, or otherwise unable to support standard tools or service requirements, then we may be unable to deliver some or all of the Services. Any remediation, replacement, reconfiguration, upgrade, or additional labor required to bring a firewall appliance into compliance with these requirements is outside the scope of the Services unless expressly stated otherwise in writing.
Identity Threat Detection and Response (ITDR)	Implementation of an ITDR solution that leverages endpoint and identity telemetry to help prevent privilege escalation before damage can occur. • Correlates user, endpoint, and network behaviors to identify compromised accounts and malicious insider actions. • Disables compromised Microsoft accounts or Microsoft 365 users and isolates affected endpoints. • Monitors for stolen credentials.

	Note: For this service to run effectively, we must have administrative access, including permissions to read sign-in/audit logs and apply policy changes. If Customer has an internal IT team (such as in a co-managed situation), the internal team must not prevent us from having the administrative access described above. In addition, multi-factor authentication must be implemented and used, with no shared accounts. All users must complete enrollment and refrain from reusing passwords and sharing credentials. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed Detection & Response (MDR)	Implementation and facilitation of a top-tier MDR solution from our designated Third-Party Provider. • 24x7 Managed network detection and response. • Real time and continuous (24x7) monitoring and threat hunting. • Real time threat response. • Alerts handled in accordance with our Service response times, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request. • 24x7x365 access to a security team for incident response* * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Managed 365 Security Operations Center (SOC)	This service focuses on Client's Microsoft 365 environment. The service includes continuous monitoring of Microsoft 365 security events, alerts, logs, identities, email activity, collaboration activity, and related telemetry; alert triage; investigation of suspected threats; threat hunting; incident escalation; and response coordination or response actions. Please note: Managed 365 SOC is designed to improve visibility into threats affecting Microsoft 365, but it does not guarantee that all threats, attacks, unauthorized activity, or policy violations will be detected, prevented, or remediated. For this service to work most effectively, Client must promptly review and respond to alerts, recommendations, and incident notifications delivered by us whenever Client action, confirmation, or approval is required; and notify us promptly of any material changes to Client's Microsoft 365 tenant, licensing, users, domains, integrations, identity provider, email configuration, security settings, or related systems that could affect the Managed 365 SOC services. * **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Microsoft 365 Cloud Backup	Implementation and facilitation of a cloud to cloud backup solution from our designated Third-Party Provider. Our cloud-to-cloud Microsoft 365 backup service protects your critical business data by securely backing up Microsoft 365 to an independent cloud environment. This ensures your emails, files, and collaboration data are recoverable even if they are accidentally deleted, corrupted, or impacted by cyber incidents. All cloud backups will be stored in a secure data center. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis. Features include: • Automated cloud-to-cloud backups for Microsoft 365 • Coverage for Exchange, OneDrive, SharePoint, and Teams • Secure, independent cloud storage with encryption

	• Fast search and granular restore (single items or full accounts) • Point-in-time recovery and long-term retention • Protection from accidental deletion, ransomware, and data loss • Compliance and e-discovery support • Scalable, fully managed service
Mobile Device Management (MDM)	Centralized, cloud-based management of company devices and business applications. This service helps standardize device configurations, enforce security controls, protect company data, and support remote and hybrid users across various mobile devices. Devices enrolled in MDM can be remotely patched, configured, and monitored for usage controls and license management, and can communicate acceptable use expectations to end users and obtain required consents. Enrolled devices can also be remotely locked or wiped in the event they are lost or stolen. Note: This service is a management and policy enforcement tool, not a guarantee of security. Effectiveness depends on device supportability, user behavior, and compliance with required configuration settings. It is the Customer's responsibility to (i) approve which users/devices are eligible for MDM service enrollment, provide us with timely decisions on security policies and exceptions, and to notify us immediately in the event an enrolled device is lost or stolen.
Multi-Factor Authentication	Multi-Factor Authentication ("MFA") adds an additional layer of security to user logins by requiring more than one method of verification, typically something the user knows (a password) and something the user has (an authentication app, mobile device, token, or code). MFA substantially reduces the likelihood of unauthorized access caused by weak, stolen, or compromised passwords. **MFA Configuration & Deployment:** We will assist with the initial configuration and deployment of an MFA solution from our designated third-party provider. **Policy & Enforcement Settings:** We will configure applicable MFA enforcement settings consistent with security best practices, including conditional access rules where supported. **User Enrollment Support:** We will provide remote guidance during the MFA setup process (*e.g.*, installing an authenticator app, enrolling a mobile device, scanning QR codes, etc.). **Ongoing Administration:** We will assist with MFA-related administrative tasks such as device resets, re-enrollment, and verification-method updates, subject to Client approval. **Client Responsibilities** For MFA to function properly and consistently, Client must: • Ensure each user has access to a compatible authentication method (e.g., smartphone, token, or approved device). • Ensure users safeguard their authentication device, including maintaining password/PIN protection on mobile devices. • Immediately notify us if a user's authentication device is lost, stolen, compromised, or replaced. • Ensure users complete enrollment steps promptly when instructed. • Ensure that users comply with all MFA policies, enforcement rules, and security recommendations that we provide to Client or its staff.
	This service focuses on the entire managed network, observing traffic patterns and communications to identify potential security threats. It analyzes network traffic using

Network Detection & Response (NDR)	analytics, machine learning, and artificial intelligence (AI) to recognize patterns associated with malicious behaviors. This service continuously scans network data to detect threats that have bypassed traditional perimeter security measures like firewalls and intrusion prevention systems. Features include: • Analyzes Network Traffic. Analyzes raw network traffic and metadata, monitoring both north-south (external) and east-west (internal) traffic. This ensures visibility into suspicious activities like lateral movement, privilege escalation, and unusual data transfers. • Detects Behavioral Anomalies. Using machine learning models, the service establishes a baseline of normal network behavior and detects deviations that may indicate potential threats. • Analyzes Encrypted Traffic. This service analyzes encrypted traffic patterns without decrypting the data, leveraging metadata and flow characteristics to identify threats while preserving privacy and compliance. **Customer Responsibilities**: For this service to run effectively, we must have administrative access, including permissions to read sign-in/audit logs and apply policy changes. If Customer has an internal IT team (such as in a co-managed situation), the internal team must not prevent us from having the administrative access described above. * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
New Employee Provisioning	New Employee Provisioning is the standardized process by which we configure and deploy all required technology resources for a customer's new personnel, ensuring secure, consistent, and timely onboarding aligned with the client's operational and security requirements. This service includes: • **User Account Setup:** Creation and configuration of user accounts across supported systems, including directory services (*e.g.*, Active Directory / Microsoft 365), email, and line-of-business applications. • **Access & Permissions Assignment:** Implementation of role-based access controls (RBAC) based on information provided by the customer, ensuring the new user has appropriate access to systems, files, and applications necessary for their role. • **Device Preparation & Configuration:** Setup and deployment of desktops, laptops, and/or mobile devices, including installation of required software, security tools, and endpoint management agents. • **Security Configuration:** Enforcement of baseline security protocols, including multi-factor authentication (MFA), password policies, endpoint protection, encryption, and compliance with the customer's security policies. • **Email & Collaboration Tools:** Provisioning of email accounts, distribution lists, shared mailboxes, and collaboration tools (*e.g.*, Teams, SharePoint, or equivalent platforms). • **Licensing Assignment:** Allocation and configuration of software licenses as directed by the customer or in accordance with the agreed licensing plan. • **Documentation & Tracking:** Recording of provisioning activities within our ticketing and documentation systems to ensure auditability and consistency. For this service to be implemented effectively, the customer must provide complete and accurate onboarding requests, including: ○ Employee name and start date ○ Role/title and department ○ Required systems and access levels In addition, the customer must:

	• submit provisioning requests with sufficient lead time; • approve access levels and licensing requirements; and • ensure compliance with internal HR and security policies.
Password Manager	Implementation and facilitation of a password management protection solution from our designated Third-Party Provider. • Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Financial Information Vault: Securely store and organize financial information such as bank accounts and credit card information in a secure digital location accessed through your browser or an app. • Contact Information Vault: Store private addresses and personal contact information within your vault accessed through your browser or an app. • Browser App: Browser extension permits easy access to your information including the vaults, financial information, contact information, and single sign-on through the app. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device.
Penetration (Pen) Testing	Penetration testing (or "pen" testing) simulates a cyberattack against your IT infrastructure to identify exploitable vulnerabilities. Unlike ongoing vulnerability scanning services that provide a constant, static level of network scanning, pen testing may involve several stages of reconnaissance and actual attack methodologies (such as brute force attacks and/or SQL injection attacks) and may include unconventional and targeted attacks that occur during business and non-business hours. Pen testing may consist of any of the following: **External Pen Testing:** exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access. **Internal Pen Testing:** Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained. **PCI Pen Testing:** Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies. **Web App Pen Testing:** Application security testing using attempted infiltration through a website or web application utilizing PTES and the OWASP standard testing checklist. Please see additional terms for Penetration Testing below.
Privileged Access Management ("PAM")	This service is designed to reduce the risk of unauthorized access, ransomware, and insider misuse by controlling and monitoring administrative ("privileged") access to your managed systems and applications. PAM helps ensure that elevated access is granted only to authorized users, for approved purposes, and only for the time necessary to perform the required task. As part of this service, we may: • Identify and inventory privileged accounts (including administrative accounts, privileged groups, and service accounts) within the in-scope environment.

	• Implement least-privilege controls to reduce or eliminate persistent administrative access where feasible. • Secure privileged credentials using controlled storage and access procedures (e.g., vaulting and managed access workflows), as applicable to the selected PAM solution. • Provide time-limited ("just-in-time") privileged access, including approval workflows, where supported and where configured by Customer. • Monitor and audit privileged activity, including maintaining logs of privileged access events and, where enabled, privileged session monitoring/recording. • Automate credential rotation for in-scope privileged accounts where supported (e.g., rotating administrative passwords on a scheduled basis and/or after use). • Support incident-driven response actions relating to privileged credentials, such as forced password resets, revoking privileged access, and accelerating credential rotation when compromise is suspected. Important: PAM reduces risk but does not eliminate it. Effectiveness depends on the completeness of deployment, Customer participation, and the security posture of the broader environment. For this service to run effectively, we must have administrative access, including permissions to read sign-in/audit logs and apply policy changes. If Customer has an internal IT team (such as in a co-managed situation), the internal team must not prevent us from having the administrative access described above.
Quarterly Business Reviews (QBRs)	QBRs are recurring strategic meetings intended to review the overall status, performance, alignment, and direction of the Services as well as Client's managed IT environment. The purpose of the QBR is to provide a structured opportunity for us to discuss trends, recurring issues, business objectives, technology planning, security matters, service performance, and other items relevant to our relationship with you. The effectiveness of a QBR depends on Client's preparation, and consistent attendance and participation. **We strongly advise you to attend all scheduled QBRs. Non-attendance may limit our ability to address key topics related to the Services and could hinder us from offering you the latest service options available.** If Client cancels, reschedules, or fails to attend a scheduled QBR on more than one occasion, we may treat the missed session as delivered for that quarter or may reschedule the QBR as our availability permits.
Remote Helpdesk	**End-User Support (L1/L2 Assistance)**: Remote assistance for day-to-day technical issues affecting Client's managed IT environment. Support is limited to issues involving software that is acquired through ICS; any other software assistance, if provided, is on a "best efforts" basis with no guarantee of resolution. **Incident Logging & Ticket Processing**: Service requests are logged, categorized, and prioritized. Response and resolution times are subject to the Service Levels described in this Guide, and are not guaranteed unless expressly stated as such. **Remote Troubleshooting**: We may use remote access tools to diagnose and remediate issues. Remote support is contingent on the availability of a stable internet connection, functioning remote-access agents, and appropriate user authorization. **Password Resets & Basic Account Assistance**: Upon request, we will perform password resets and related account unlock services for supported authentication systems. **Email & Productivity Application Support**: We will provide support for standard functions within Microsoft 365, Google Workspace, and other applications licensed through ICS. We will also provide support for most line-of-business applications, regardless of whether they are acquired through ICS; however, such support is on a "best efforts" basis with no guarantee of issue resolution. Support does not include custom configurations, scripting, complex data migrations, or development work.

	Workstation and Peripheral Assistance: We will assist remotely with basic configuration of supported devices and peripherals. Physical repairs, on-site adjustments, cabling issues, or hardware replacements are excluded unless separately contracted. **Network Connectivity Assistance**: We may assist with basic Wi-Fi, VPN, and network connectivity issues affecting the managed IT environment. We are not responsible for ISP outages, environmental interference, building wiring, or Client-owned network equipment not under a separate management plan. **Hardware-Related Support (Remote Only)**: We may diagnose potential hardware failures remotely. We are not required to open devices, perform repairs, replace components, or dispatch technicians unless separately contracted. **How-To Guidance**: We may provide short, informal guidance on the use of supported software and features. Such guidance does not include formal training, user education programs, or professional instruction. **Periodic Service Reports**: Upon request, we can provide Client with service performance summaries.
Remote Monitoring and Management (RMM)	RMM is the remote monitoring, alerting, and management process we use to help maintain the health, availability, and performance of the covered servers, workstations, and other supported devices in the Environment ("Covered Equipment"). As part of this service, we deploy software agents or other management tools to Covered Equipment. These tools report system status, device health, operating conditions, and certain IT-related events on an ongoing basis. Alerts generated through these tools are reviewed and addressed in accordance with the applicable service levels, response procedures, and scope of services described in the Quote and this Guide. RMM helps us identify and respond to common technology conditions before they become more serious operational issues. Depending on the Covered Equipment, selected service plan, and supported configuration, RMM may include monitoring and management of device availability, disk capacity, operating system health, patch status, backup status, agent status, uptime, and other system conditions. RMM may also include the following activities: • Monitoring covered systems for defined alerts, events, and health conditions. • Reviewing alerts generated by supported monitoring tools. • Monitoring disk capacity on supported fixed internal drives and standard system partitions. • Performing routine operating system health checks and maintenance activities intended to reduce common performance or disk-space issues. • Reviewing and deploying applicable updates and patches for supported operating systems and supported software. • Monitoring whether required management agents are installed, active, and properly reporting. • Monitoring selected backup-related alerts where backup services are included in the applicable service plan. • Identifying devices that are offline, not reporting, or otherwise unavailable to our management tools. • Performing scheduled reboots or recommending reboots where excessive uptime may affect stability, patching, or performance. • Documenting or escalating conditions that require customer approval, third-party vendor involvement, hardware replacement, software licensing, or project work. RMM is not intended to detect every possible failure, security event, vulnerability, configuration issue, performance issue, application problem, or user-created condition.

	The effectiveness of RMM depends on the Covered Equipment being powered on, connected to the internet, properly licensed, supported by the applicable vendor, accessible by our tools, and not altered in a way that interferes with monitoring or management. Unless expressly stated otherwise, RMM does not include monitoring of unsupported devices, external drives, USB drives, mapped drives, removable media, personally owned devices, unauthorized software, end-of-life systems, systems outside the agreed scope, or devices on which the required management tools cannot be installed, maintained, or monitored.
Security Hardening & Risk Management	Security Hardening and Risk Management Services consist of measures designed to improve the security posture of Client's IT environment by reducing vulnerabilities, limiting unnecessary exposure, and supporting the identification and management of material technology-related risks. These Services include vulnerability scanning (described in this Guide, below), device encryption (described in this Guide, above), the review and adjustment of system configurations, implementation of security baselines, disabling unnecessary services or access pathways, strengthening authentication and access controls, assisting with patching practices, reviewing administrative privileges, and making commercially reasonable recommendations intended to align Client's environment with generally accepted security practices.
Security Incident & Event Monitoring (SIEM)	Implementation and facilitation of an industry leading SIEM solution from our designated Third-Party Provider. The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network. ➢ Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the "Initial Assessment"). ➢ Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack. • Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an "Event"), then you will be notified of that Event. Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the "Criteria"). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client's environment and user behavior. During this initial thirty (30) day period, Client may experience some "false positives" or, alternatively, during this period not all anomalous activities may be detected. Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats is not within the scope of this service and may require Client to retain ICS's services on a time and materials basis.
Server Monitoring & Maintenance	As part of our RMM service, we will monitor and maintain managed servers as follows: • Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

	• Online status monitoring, alerting us to potential failures or outages • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) • Performance monitoring, alerting us to unusual processor or memory usage • Server essential service monitoring, alerting us to server role-based service failures • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities • Routine operating system inspection and cleansing • Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection
Technical Alignment Management	Our Technical Alignment Manager performs regular technical alignment reviews, validates that key configurations and controls remain in place, identifies technical risk, and ensures your environment is documented in a way that supports efficient support and long-term planning. • Standards Library Governance: We develop and maintain a standards library (best practices) and update it as technology and requirements change, typically with input from a cross-functional standards committee. • Scheduled Alignment Reviews: We perform periodic alignment visits based on your environment's size/complexity (commonly monthly, quarterly, semi-annual, etc.). Visits are scheduled and managed as part of the ongoing service. • Alignment Assessment + Documentation: We validate your environment against objective standards, record what is aligned/misaligned, and maintain the technical documentation necessary to support efficient service delivery. • Risk & Remediation Identification: Misalignments and technical risks are identified and translated into clear remediation recommendations and action items for follow-up. • Operational Handoff to Strategy (vCIO): Findings are provided to the vCIO as inputs for planning, prioritization, and roadmap discussions so recommendations are tied to outcomes and executed through appropriate delivery teams.
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. Please note: We 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. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.
Virtual Chief Information Officer (vCIO)	Act as the main point of contact for certain business-related IT issues and concerns. • Assist in creation of information/data-related plans and budgets. • Provide strategic guidance and consultation across different technologies.

	• Create company-specific best standards and practices. • Provide education and recommendations for business technologies. • Participate in scheduled meetings to maintain goals. • Maintain technology documentation. • Assess and make recommendations for improving technology usage and services. Note: This service does not guarantee any specific business, financial, operational, security, or compliance outcomes. Recommendations are advisory only and are based on information provided by Client. Client retains all authority and responsibility for final decisions, budget approvals, policy adoption, risk acceptance, and operational execution. Through this service, we are not acting as a fiduciary, officer, director, or employee of the Client. Our vCIO services do not create any fiduciary, agency, or employer/employee relationship.
Voice Over IP (VoIP) Services	Implementation and facilitation of an industry-recognized VoIP solution from our designated Third-Party Provider. Features include: • Scalable VoIP-based telephone service with call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities. • Central control panel provides access to VoIP-related configurations, including physical address registration, call routing, updating greetings, and ability to turn on/off service features. • Ability to use mobile app dialing **Important**: There are additional terms related to the VoIP service, including your use of E911 features, toward the end of this Services Guide. Please read them carefully. You may be required to sign an additional consent form indicating your understanding and acceptance of the limitations of 911 dialing using the VoIP services.
Vulnerability Scanning	Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third-Party Provider. Vulnerability scanning identifies holes in the managed network that could be exploited. External vulnerability scans (which pertain to the IP address assigned to each customer location through the Client's ISP) are run monthly. Internal vulnerability scans (which pertain to all systems inside the managed network) are run at least annually. Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request. Please see additional terms for vulnerability scanning below.
Wi-Fi Services	ICS will install at the Client's premises Wireless Access Points to provide bandwidth in all areas requiring wireless network coverage, as agreed upon by ICS and Client. • ICS will maintain, supervise, and manage the wireless system at no additional cost. • Installed equipment, if provided by ICS, will be compatible with the then-current industry standards. • ICS will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well).

	Please note: Any Wi-Fi devices, such as access points or routers, which are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).
Workstation Monitoring & Maintenance	Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives). • Performance monitoring, alerting us to unusual processor or memory usage. • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software. • Asset inventory and workstation information collection.

Project-Related Services

For project-based services, one-time or limited-time engagements, or similar engagements listed in a Quote ("Projects"), the following provisions shall apply:

- All our labor will be billed to you at our then-current hourly rate in fifteen (15) minute increments, with partial increments being rounded to the next highest increment.
- Project-related services will be performed during normal work hours only. If Project work is required to be performed after-hours or during non-business hours, our hourly rates will be increased as per the table below for the time expended in off-hours or non-business hours.
- You agree to reimburse us for all reasonable and pre-approved travel costs and expenses that are directly attributable to, or are reasonably required to be incurred, while providing Project-related services. ICS reserves the right to require pre-payment of anticipated travel costs and expenses.
- Our current hourly rates are $100 - $125. Rates will be multiplied by one and one-half times (1.5x) for after-hours or non-business work hours.

Block of Hours / Allocated Consulting Hours

If you purchase one or more blocks of technical support or consulting hours from us, then we will provide our professional information technology consulting services to you from time to time on an ongoing, "on demand" basis ("Services"). The specific scope, timing, term, and pricing of the Services (collectively, "Specifications") will be determined between you and us at the time that you request the Services from us.

You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an "Invoice"), or in some cases, (iii) by us performing the Services or delivering the applicable deliverables in conformity with the Specifications.

If we provide you with an email or an Invoice that contains details or terms for the Services that are different than the terms of the Quote, then the terms of the email or Invoice (as applicable) will control for those Services only.

A Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications ("Service Completion"). (For example, sales of hardware will be deemed completed when the hardware is delivered to you; licensing will be completed when the licenses are provided to you, etc.) Any defects or deviations from the Specifications must be pointed out to us, in writing, within ten (10) days after the date of Service Completion. After that time, any issues or remedial activities related to the Services will be billed to you at our then-current hourly rates.

Unless we agree otherwise in writing, Services will be provided only during our normal business hours. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement.

The priority given to implementing the Services will be determined at our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from us. If no specific milestone or deadline is agreed upon, then the Services will be performed in accordance with your needs, the specific requirements of the job(s) and technician availability.

On-Premise Personnel

On-premise personnel services apply to situations in which we locate one or more of our employees at your business location to provide dedicated or semi-dedicated technical support resources. These resources may assist with services identified in an applicable Quote or as otherwise directed by ICS, which may include end-user support, troubleshooting, ticket handling, device setup, coordination with remote support teams, basic systems administration, technology documentation, and other activities. If additional services are required, you must call us to arrange for those services; the scope of ICS's personnel's activities is defined solely by ICS. **On-premise personnel may provide technical assistance and recommendations, but they are not responsible for making Client business decisions, approving purchases, managing Client employees, or assuming operational roles unless ICS expressly agrees upon such services in writing.**

This service is intended to facilitate technical services, enhance operational visibility, and if applicable, facilitate direct interaction between Client's personnel and our offsite technical team. All on-premise personnel are, and will remain at all times, ICS's employees, and these services do not create an employment, co-employment, leased employee, staff augmentation, or agency relationship with ICS or any of the on-premise personnel. Client may provide reasonable direction regarding service priorities, site access, and business needs within the scope of services (as described above), but Client shall not supervise, discipline, manage, hire, terminate, or otherwise exercise employer-level control over our personnel.

These services are provided during our normal business hours only, and are provided in blocks of hours that are pre-purchased by Client. Our personnel must be given free access to the premises in which they are requested to work. Our personnel will comply with Client's reasonable site rules, security procedures, and safety policies, provided those rules are disclosed in advance and do not conflict with our employment policies, the Quote, this Guide or the MSA.

Unless we agree otherwise in writing, we may replace, rotate, reassign, or substitute personnel as needed. Client may request replacement of a resource for legitimate performance, security, or business reasons, but ICS retains final staffing authority.

On-premise personnel may provide technical assistance and recommendations, but they are not responsible for making Client business decisions, approving purchases, managing Client employees, or assuming operational roles unless expressly stated in writing.

Physical Implementation of Equipment

The provisions in this section apply to all services in which we install or implement equipment, including cameras, access points, cabling, sensors, door access devices, racks, mounts, or similar onsite equipment ("Implementation Services").

- **Procurement**. We will procure the equipment listed in the applicable Quote. If selected equipment becomes commercially or practicably unavailable, we may substitute other equipment that is the equivalent or better.
- **Pre-Installation Planning**. Depending on the installation requirements, we may conduct one or more pre-installation planning meetings with you to determine and finalize the locations at which equipment will be installed. After these meetings you will be requested to approve the installation plans. Once you approve of the plans, the installation plans will be deemed final; any material deviations from the approved plans thereafter will require a change order. You will be responsible for selecting and approving the final location, mounting height, viewing angle, field of view, and intended purpose of each camera or device (if applicable). We may offer general recommendations, but you will remain responsible for determining whether the selected locations satisfy your specific operational, security, privacy, legal, and regulatory requirements.
- **Site Readiness**. You will be responsible for ensuring that all installation locations are reasonably accessible, structurally suitable, properly powered, network-ready, and otherwise prepared for the scheduled services. Delays, return visits, additional labor, or additional materials caused by lack of site readiness may be billed as additional services.
- **Permits**. Unless local law requires us to do so or unless otherwise stated in an applicable Quote, you will be responsible for identifying and obtaining any permits, landlord approvals, association approvals, building access permissions, security clearances, licenses, inspections, or governmental approvals required for the installation or use of the equipment.
- **Exclusions**. Unless expressly stated in the applicable Quote, Implementation Services do not include electrical work, construction, demolition, conduit installation, ceiling or wall repair, painting, permitting, structural engineering, or hazardous material remediation.
- **Environmental Factors**. Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances, or that installed camera or recording equipment will prevent crime, loss, injury, or other adverse events.
- **Privacy**. You are solely responsible for ensuring that your use of cameras, microphones, video analytics, recording functions, facial recognition, motion detection, and related technologies complies with all applicable laws, including privacy, wiretapping, employment, consumer protection, biometric, landlord-tenant, and surveillance laws. Provider does not provide legal advice regarding the legality of any recording, monitoring, retention, notice, or disclosure practice. You will not request or require us to install cameras or recording devices in areas where

individuals have a reasonable expectation of privacy. Unless expressly included in the applicable Quote, we will not enable audio recording in installed cameras or microphones. If you request that audio recording be enabled, you will be solely responsible for determining whether such recording is lawful and for obtaining all required notices, consents, authorizations, and signage.

- **Damage to Premises**. We will use commercially reasonable care when performing Implementation Services. You acknowledge that physical installation may involve drilling, mounting, cabling, fastening, moving ceiling tiles, accessing walls or ceilings, or similar activities that may cause minor cosmetic impacts. We are not liable for preexisting damage, hidden conditions, normal installation impacts, or damage resulting from Customer-provided instructions, unsuitable surfaces, or third-party work. Similarly, we are not liable for preexisting defects, undocumented configurations, unsupported systems, or failures caused by existing infrastructure that is inadequate, defective, misconfigured, or not disclosed to us.
- **Change Orders**. Any work outside the stated scope, including additional devices, different mounting locations, longer cable runs, after-hours work, return visits, lift rental, additional materials, troubleshooting preexisting issues, or changes requested after installation begins, may require a change order or may be billed as additional services.

Hardware as a Service (HaaS)

The provisions below apply to all hardware, devices, and accessories that are provided to you on a "hardware as a service" basis.

- **Scope**. Provision and deployment of hardware and devices listed in the Quote or other applicable schedule ("HaaS Equipment").

- **Deployment**. We will deploy the HaaS Equipment within the timeframe stated in the Quote, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guaranty does not apply to any software, other managed services, or hardware devices other than the HaaS Equipment. In addition, this deployment time frame may be extended as necessary to accommodate delays that are outside of our reasonable control, such as embargoes, labor or supply chain shortages, or other force majeure events.

- **Delayed Deployment**. If you wish to delay the deployment of the HaaS Equipment, then you may do so if you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote. You will be charged at the rate of fifty percent (50%) of the monthly recurring fees for the HaaS-related services during the period of delay. Following deployment, we will charge you the full monthly recurring fee (plus other usage fees as applicable) for the full term indicated in the Quote.

- **Repair/replacement of HaaS Equipment**. ICS will endeavor to repair or replace HaaS Equipment within five (5) business days following the business day on which the applicable problem is identified by, or reported to, ICS and has been determined by ICS to be incapable of being remediated remotely. This warranty does not include the time required to rebuild your system, such as the time required to configure a replacement device, reload the operating system, reload and configure applications, and/or restore from backup (if necessary).

- **Technical Support for HaaS Equipment**. We will provide technical support for HaaS Equipment in accordance with the Service Levels listed in this Services Guide.

- **Usage**. You will use all HaaS Equipment for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the HaaS Equipment available to any third-party without our prior written consent. You agree to refrain from using the HaaS Equipment in a manner that unreasonably or materially

interferes with our other hosted equipment or hardware, or in a manner that disrupts or that is likely to disrupt the services that we provide to our other clientele. We reserve the right to throttle or suspend your access and/or use of the HaaS Equipment if we believe, in our sole but reasonable judgment, that your use of the HaaS Equipment violates the terms of the Quote, this Services Guide, or the Agreement.

- **Return of HaaS Equipment**. Unless we expressly direct you to do so, you shall not remove or disable, or attempt to remove or disable, any software agents 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 we remediate the situation at our 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 ICS access to the premises at which the HaaS Equipment is located so that all such equipment may be retrieved and removed by us. If you fail to provide us with timely access to the HaaS Equipment or if the equipment is returned damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Policies and Procedures Applicable to Services

Software Licensing: All software provided to you by or through ICS is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in ICS's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.

When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

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

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

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

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis only and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation.

Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation and not an obligation to you.

If we are unable to remediate an issue with non-Supported Software, then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software and if you have a Service Contract in place, our facilitation services will be provided to you at our then-current hourly rates.

Physical Locations Covered by Services. Services will be provided remotely unless, at our discretion, we determine that an onsite visit is required. ICS visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

Evolving Technologies: Technologies can evolve rapidly. In certain instances, depending on the scope and timing of an applicable service, technologies comprising or included in a service may evolve before the service can be fully implemented. Should this occur, we will provide you with options to leverage the latest version of the evolved technology and inform you of the attendant fees and costs to do so. If you decline to implement the evolved technology, then we will continue to implement the service as indicated in the Quote; however, you understand and agree that (i) you will not benefit from improvements in the evolved technology, and (ii) the applicable technology and service may become obsolete more quickly.

Minimum Requirements / Exclusions. The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be provided/maintained by Client at all times:

- Server hardware must be under current warranty coverage
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed, and vendor- or OEM-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Client must provide us with exclusive administrative privileges to the Environment.

- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

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 ICS**. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by ICS in writing:

- Customization of third-party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels. Automated services are provided on an ongoing (*i.e*., 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 8:00 AM – 5:00 PM Central Time, excluding legal holidays and ICS-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by ICS in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; ICS 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	Response Time
Critical / Service Not Available (*e.g*., all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g*., large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g*., limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.
Small Service Degradation (e.g., business process can continue, one user affected).	Response within two (2) business days after notification.
Long Term Project, Preventative Maintenance	Response within four (4) business days after notification.

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

Support During Off-Hours/Non-Business Hours: Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If ICS agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at the rates (and hourly multipliers) indicated in the table in "Project-Related Services," above.

ICS-Observed Holidays: ICS observes the following holidays:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Christmas Eve Half Day
- Christmas Day

Service Credits: Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing (as per the requirements of our Master Services Agreement), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

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

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

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

Travel Time. If onsite services are provided for managed services, we will travel up to 45 minutes from our office to your location at no charge. Time spent traveling beyond 45 minutes (*e.g.,* locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

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

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

Term; Termination. The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to ICS's satisfaction.

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

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

Removal of Software Agents; Return of Firewall & Backup Appliances: Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the managed environment or any of the devices on which we installed software agents. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, you must remove, package and ship, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise provided to you by ICS "as a service." If you fail to timely return all such equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Offboarding. Offboarding is intended to help facilitate an orderly transition of supported systems, documentation, administrative access, and applicable service responsibilities to a provider other than ICS. Subject to the requirements,

conditions, and limitations set forth in the MSA, we will assist you with the transition away from our managed services through an offboarding process that is mutually coordinated between you and us.

Offboarding will be performed under a transition plan agreed upon by you and us. The transition plan may identify the applicable timeline, systems to be transitioned, information to be provided, credentials or administrative access to be transferred or disabled, software tools to be removed, vendor responsibilities, communication procedures, and any remaining tasks that must be completed before the Services end.

We strongly recommend that, for transition purposes, you overlap the Services with the services of any incoming provider for at least one full calendar month. This overlap period helps reduce the risk of gaps in monitoring, management, backup, cybersecurity, patching, vendor support, documentation transfer, user support, and other critical services. A transition without an adequate overlap period may result in delays, missed alerts, loss of visibility, incomplete handoff, service interruptions, or other avoidable issues.

You will be responsible for ensuring that your incoming provider cooperates with us during the offboarding process and follows our agreed-upon transition plan. **Unless we otherwise agree in writing, neither you nor your incoming provider may disable, uninstall, remove, alter, or interfere with any software agents, monitoring tools, security tools, remote access tools, backup tools, management agents, or other ICS-deployed software or configurations installed or implemented in the Environment**. Unauthorized removal or alteration of those tools may interfere with our ability to provide Services (including offboarding services).

If you or your incoming provider removes, disables, alters, or interferes with ICS-installed tools without our prior consent, you will be solely responsible for any resulting issues, service disruption, loss of monitoring, loss of management capability, security exposure, data loss, remediation work, vendor charges, licensing fees, investigation time, reinstallation costs, or other costs and fees incurred by us or you. We will have no responsibility or liability for conditions caused by unauthorized changes made by you, your personnel, or your incoming provider.

.

Additional Policies

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

Authenticity

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by ICS, and Client shall not modify these levels without our prior written consent.

Configuration of Third-Party Services

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

Modification of Environment

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

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that ICS 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 our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data or systems impacted by the incident will be recoverable or remediated. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported

by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other 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—including ours. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third-party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by ICS 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. ICS 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 ICS believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Backup (BDR) Services

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

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

Procurement

Equipment and software procured by ICS 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, ICS 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. ICS is not a warranty service or repair center. ICS 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 ICS will be held harmless, and (ii) ICS 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.

Business Review / IT Strategic Planning Meetings

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

VCTO or VCIO Services

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

Sample Policies, Procedures.

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

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

No Third-Party Scanning

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

Obsolescence

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

Licenses

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

VoIP-Related Policies/Requirements

VOIP – Dialing 911 (Emergency) Services

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

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

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

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

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

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

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

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

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

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

Messaging: All messages sent through the VoIP service must conform to the following requirements and restrictions:

- Recipients must give their consent to receive text messages from you. This can be direct consent or, depending on the circumstances, implied consent (such as a pre-existing business relationship, contact initiated by the recipient, etc.).
- Recipients must be provided with an opt-out mechanism to avoid receiving future text messages from you.
- You shall not mis-identify yourself or cause the message to appear as if it was sent from a telephone number other than the number assigned to you by the VoIP service.
- All messaging-related activities must strictly comport with the requirements and restrictions of the Telephone Consumer Protection Act (47 USC §227) ("TCPA"). You agree to indemnify and hold us harmless from any costs, fees, expenses, and/or penalties that we incur because of your failure to abide strictly by the TCPA. If, in our reasonable judgment, we believe that your activities violate the TCPA, we reserve the right to suspend the messaging service until we receive reasonable assurances that the activity has stopped and will not be repeated. Repeated violation of the TCPA is a material breach of your agreement with us.

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

AI-Enabled Services
Privacy & Use Disclosure

This Disclosure describes how certain services implemented or facilitated by ICS use artificial intelligence ("AI")-based technologies and how data processed through those services is collected, managed, and used.

AI Deployment

AI-driven tools and technologies ("AI Tools") may be included in certain third-party services we facilitate or implement for you. Depending on the services, AI Tools may be used to help enhance efficiency, automate tasks, analyze information, and provide you with advice, strategies, and insights about your business operations, your managed information technology ("IT") infrastructure, and/or how to automate time-consuming tasks to enhance efficiency and productivity.

We strive to offer Services that incorporate AI Tools managed by reputable third-party providers who represent that their AI technologies are used solely for the specific, authorized tasks for which they are designed, and for no other purpose.

Use of Data

The AI Tools are developed and maintained by third-party providers. To the best of our knowledge (except as otherwise stated below), these AI Tools do not access or use your data for any reason other than to perform the specific and authorized functions for which they have been implemented. Virtually all third-party AI Tools process data in an anonymized and de-identified manner to enhance or improve the algorithms, systems, or overall performance of the AI platform. The anonymization/de-identification process strips processed data of all personal information as well as any information that could be tracked back to you or the applicable data subject, protecting privacy while preserving data utility for training or analysis.

Most often, this process cannot be avoided and, therefore, you should expect that part or all of your data may be anonymized, de-identified, and subsequently used by the AI Tools for training and analytical purposes. If we are given the ability to modify the privacy settings of the AI Tools accessed through the services, we will select the most restrictive settings to help ensure that your data is not used for any purposes other than stated in this Disclosure.

Shared Risk

As with any emerging technology designed to deliver advanced strategies and operational efficiencies, AI may sometimes act in unpredictable ways or produce results that differ from the intended purpose. There is also the possibility that one or more third parties that develop or maintain the AI tools could fail to comply with their stated privacy policies or with applicable data-security standards, which could result in data leakage or unauthorized disclosure.

While these risks are considered low, they are not nonexistent. We believe that the benefits, efficiencies, and overall advantages of using the services that use AI Tools significantly outweigh the relatively small risks described above. Accordingly, unless we have actual knowledge that a specific AI Tool or its provider fails to maintain generally accepted privacy or data-security practices, we will not monitor, restrict, or otherwise interfere with the operation of any Service that includes such AI tools.

If we become aware of an ongoing privacy or security issue associated with any AI tool, we may modify the affected services to remove or disable that tool.

By using the services, you acknowledge the inherent risks associated with the AI Tools and agree that ICS will not be liable for any AI Tool-related act, omission, or outcome that is outside our control.

You are also advised as follows:

- You should independently evaluate and verify the accuracy, relevance, and suitability of any AI Tool-generated advice, recommendation, or strategy before relying upon it;
- You are the final decision maker regarding whether to adopt, reject, or modify any AI Tool-generated result or strategy; and,
- We make no representation or warranty that AI Tool-generated results will be correct, complete, or fit for your intended purpose.

Inquiries

You may request additional information about the AI Tools by sending us an email at info@chooseics.com.

Vendor-Specific Policies Applicable to the Services

To the extent that the Services include or use any of the third-party solutions listed in the table below, you understand and agree that the applicable services' end user license, reseller, and/or customer agreements as listed below shall apply to your use or the Service(s).

Third-Party Solution Provider	Service	Terms
Acronis	Data Backup, Disaster Recovery	https://dl.acronis.com/u/pdf/Acronis_corporate_EULA_en-US.pdf
Adobe	PDF Software	https://www.adobe.com/legal/terms.html
Atakama	Web Filtering, URL Filtering	https://www.atakama.com/terms
Barracuda	Email Security, Backup, Network Security, Data Protection	https://www.barracuda.com/company/legal/terms-of-use
Blumira	SIEM, Threat Detection & Response, Security Monitoring	https://www.blumira.com/legal/terms-of-service/
CyberFOX (AutoElevate)	Privileged Access Management (PAM), Endpoint Privilege Management	https://cyberfox.com/legal/terms-of-service/
Cynomi	Risk & Compliance Assessments	https://cynomi.com/eula/
Datto EDR, Datto AV, Ransomware Detection Product Terms	Security	https://www.datto.com/legal/datto-edr-datto-av-ransomware-detection-product-terms/?x-craft-preview=q9T1QJysjG&token=Vb7LjyDIC1sWR2n4Q-SnVRGZskSHcIjc
Dropsuite	O365 Backup	No EULA online, but requires you to agree: • to protect all Dropsuite's (and its licensors') existing and future Intellectual Property Rights in the Dropsuite Data Backup Service; • to require the End User to use the Dropsuite Data BackUp Service (which it may either name or describe generically in its End User Terms and Conditions) only for lawful personal purposes or for its lawful internal business purposes; • to prohibit the End User from copying, reproducing, reverse-

Third-Party Solution Provider	Service	Terms
		engineering, decompiling, disassembling, reselling, distributing or modifying the Dropsuite Data Backup Service (whether named or described generically) without the written consent of the MSP, except to the extent expressly permitted by any law or treaty that is in force in the territory where that law or treaty cannot be excluded, restricted or modified, provided that where the End User seeks any such consent from the MSP, the MSP must not provide it unless and until it has sought and obtained the consent of Dropsuite to include exclusions of liability that are no less protective than the warranty exclusions set out in clause 8 of DropSuite's Online Terms of Service (https://dropsuite.com/terms/) and to include limitations on liability that are no less protective than the warranty exclusion set out in clause 10 of DropSuite's Online Terms of Service. See https://dropsuite.com/terms/ for more details. Dropsuite Retention Policy: https://help.dropsuite.com/hc/en-us/articles/22814916296215-Retention-Policy-Guide
Godaddy	Domain Registration, Web Hosting, Website Services	https://www.godaddy.com/legal/agreements
Inforcer	Microsoft 365 Security, Compliance & Policy Management	https://inforcer.com/terms-and-conditions/
IronScales	Email Protection, Cybersecurity Training	https://www.ironscales.com/hubfs/PDFs/IRONSCALES%20-%20End%20User%20License%20Agreement%20-%20April%202022.pdf
Liongard	Configuration Change Detection, Asset Discovery & Inventory	https://www.liongard.com/terms-of-use/
Microsoft Office 365		https://azure.microsoft.com/en-us/support/legal/subscription-agreement/?country=us&language=en
Microsoft applications (such as Azure Stack and individual Microsoft applications)		https://www.microsoft.com/en-us/useterms/

Third-Party Solution Provider	Service	Terms
Nerdio	Microsoft Azure Virtual Desktop Management, Cloud Management	https://getnerdio.com/legal/terms-of-use/
NinjaOne	Remote Monitoring & Management, IT Asset Management, Patch Management, Mobile Device Management	https://www.ninjaone.com/license-agreement/
Petra Security	Endpoint Protection, Security	https://commonpaper.com/standards/cloud-service-agreement/2.1
Proofpoint	Email Encryption, Spam Filtering	https://www.proofpoint.com/us/legal/license
Sangoma	VoIP Phone Systems, UCaaS, Communications	https://www.sangoma.com/legal/terms-of-service/
Sentinel One	Security	https://www.sentinelone.com/legal/master-subscription-agreement/ Also, https://www.sentinelone.com/legal/
SonicWall (all legal)	Hardware Security, Firewalls, Security	https://www.sonicwall.com/legal/end-user-product-agreements
SonicWall Managed Security Services	Security	https://www.sonicwall.com/medialibrary/legal/SonicWall-Managed-Security-Services-Terms.pdf
Splashtop	Remote Access, Remote Support	https://www.splashtop.com/terms
Syncro	PSA, RMM, Remote Monitoring & Management, Ticketing	https://syncromsp.com/terms-of-service-oct-2025
Trend Micro	Network Security	https://www.trendmicro.com/en_us/about/legal.html
Ubiquiti	Networking, Network Switches, WiFi, Security Cameras, Door Access	https://www.ui.com/eula
Veeam	Backup, Data Recovery, Storage	https://www.veeam.com/legal/eula.html
Wasabi	Cloud Storage	https://wasabi.com/legal/terms-of-use
WatchGuard	Network Security, Virtual Private Network Solutions, License Management, Identity Management	https://www.watchguard.com/wgrd-trust-center/terms-of-use

Third-Party Solution Provider	Service	Terms
WholesaleBackup (Divinsa Backup)	Cloud Backup, Disaster Recovery, Managed Backup	https://wholesalebackup.com/terms-of-service/

Additional Terms Applicable to Microsoft Products

You shall comply with the special product terms published by Microsoft for all its partners that participate in Microsoft's New Commerce Experience (NCE)/Cloud Solution Provider (CSP) reseller programs. Those product terms are located here: https://partner.microsoft.com/en-us/licensing/licensing-agreements.

If you obtain Microsoft licenses through ICS, you agree to Microsoft's terms and conditions for such licenses. This includes, but is not limited to: (a) pricing and the contract length during which that pricing is effective; (b) contract length acquired (*e.g.,* annual or monthly); (3) type of payment (*e.g.,* annual or monthly); (4) license co-terms to the annual or monthly license date for added licenses; (5) all licenses set to auto-renew unless explicitly set to not renew; (6) Microsoft's renewal date, which may differ from ICS's contractual date, in which case you shall be bound to Microsoft even after the Services terminate; and (8) your obligation to Microsoft if you terminate a Microsoft license early.

Microsoft's current contract terms are 36-months, 12-months or 30-days from license purchase date. Additional licenses can be purchased co-terminus to initial license purchase and term. During those term(s), Microsoft does not allow a decrease in license counts beyond their reduction allowance period and any termination or decrease in license counts by you shall not result in a decrease of contract costs. **You are responsible for such Microsoft charges regardless of your usage of such licenses.** ICS will make every effort to align your licenses and minimize license usage when you cooperate with such efforts, but ICS is limited by Microsoft requirements within the program and as such, you are bound to those terms and shall pay such Microsoft charges for the entire length of Microsoft's contract requirements.

Acceptable Use Policy

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

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

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

Violations of this AUP: The following constitute violations of this AUP:

- **Harmful or illegal uses**: Use of a Hosted Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.
- **Fraudulent activity**: Use of a Hosted Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.
- **Forgery or impersonation**: Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.
- **SPAM**: ICS has a zero tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC)**: The use of IRC on a hosted server is prohibited.
- **Open or "anonymous" proxy**: Use of open or anonymous proxy servers is prohibited.
- **Cryptomining:** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers**: The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agrees to allow ICS to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.
- **Email/message forging**: Forging any email message header, in part or whole, is prohibited.

- **Unauthorized access**: Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, ICS's security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.
- **IP infringement**: Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third-party, is prohibited.
- **Collection of personal data**: Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.
- **Disruptive Activity:** Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performances of our systems or networks.
- **Allowing the misuse of your account**: You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third-party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

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

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

Data Processing Policy ("DPP")

Responsibility for Processing of Personal Information

Roles: You are a Controller, and ICS is a Processor, for the Processing of Personal Information pursuant to the services provided by ICS under any Quote (the "Services").

Purposes: You and we acknowledge that the Personal Information you disclose to us is provided only for the limited and specified Business Purpose(s), and for no other reason. We will Process Personal Information solely for the purpose of providing or facilitating (as applicable) the Services.

No Additional Obligations: Unless otherwise specified in the Quote or otherwise agreed in writing by us, you shall not provide us with any data that imposes specific data security or data protection obligations on us other than those obligations specified in this DPP or a Quote. If you require additional services to address specific data security or data protection requirements applicable to your business, they must be agreed upon in writing between us and you before they can be implemented. We do not warrant or guaranty that we can or will agree to any such additional data security or data protection requirements. Until and unless we agree to provide such additional data-related services, you remain responsible for compliance with your specific regulatory, legal or industry data security obligations that apply to such data.

Restrictions: ICS will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purpose, or (ii) outside of the direct business relationship between ICS and you; or (c) combine Personal Information received from or on behalf of you with Personal Information received from or on behalf of any third-party, or collected from ICS's own interaction with Individuals, except to perform a Business Purpose permitted by applicable law and/or the applicable Quote.

We will notify you of our use of ICS Affiliates and Third-Party Subprocessors in accordance with this DPP, and we will make sure that ICS Affiliates and Third-Party Subprocessors are subject to applicable written agreements as per Applicable Law.

We will provide a level of protection to Personal Information as required by the Quote, the MSA, and Applicable Law which, in all cases, shall be a reasonable care of protection. Notwithstanding the foregoing, you may take such reasonable steps as may be necessary (a) to remediate our unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this DPP by exercising your rights under this DPP and the Services Agreement. We will notify you if we determine that we are unable to meet our privacy or confidentiality obligations.

Your Instructions

You may provide additional instructions in writing to us regarding the Processing of Personal Information in accordance with Applicable Data Protection Law. We will promptly comply with all such instructions to the extent necessary for us to (i) comply with our Processor obligations under Applicable Data Protection Law or (ii) assist you to comply with your Controller obligations under Applicable Data Protection Law relevant to your use or receipt of the Services.

We will follow your instructions at no additional cost to you and within the timeframes reasonably necessary for you to comply with your obligations under Applicable Data Protection Law. We will immediately inform you if, in our opinion, your instructions infringe Applicable Data Protection Law; however, (a) under no circumstances shall we be responsible for providing legal advice to you, and (b) no communication from us to you shall be considered to be, or relied upon as, legal advice.

Privacy Inquiries; Requests

If you receive a request or inquiry from an Individual related to Personal Information Processed by us, including an Individual's request to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, you must forward that request to our designated Privacy Officer (listed below) for follow-up. If we directly receive any inquiries from Individuals that have identified you as the Controller, we will promptly pass on such requests to you without responding to the Individual. Otherwise, we will advise the Individual to identify and contact the relevant controller(s).

ICS's Affiliates and Third-Party Subprocessors

General Authorization: You hereby provide ICS with general written authorization to engage ICS Affiliates and Third Party Subprocessors as necessary to assist in the performance and/or provision of the Services.

Requirements: To the extent we engage Third-Party Subprocessors and/or ICS Affiliates, we will require those entities to have and maintain the same level of data protection and security as ICS under the terms of this DPP and Applicable Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of our agreement with any Third-Party Subprocessors and ICS Affiliates that may Process Personal Information.

Subprocessor List: ICS maintains a list of ICS Affiliates and Third-Party Subprocessors that may Process Personal Information ("Subprocessor List"). The Subprocessor List is below, and we will provide you with an updated list throughout the term of the Services if you request us to do so in writing. Changes, if any, will automatically modify and be included in the Subprocessor List.

Objections: Within thirty (30) calendar days of us providing notice to you (as described above), you may object to the intended involvement of a Third-Party Subprocessor or ICS Affiliate by notifying us of the objection in writing. We will work together with you in good faith to find a mutually acceptable resolution to address any timely objection.

Cross-Border Data Transfers

Personal Information will be stored in our designated data storage centers in the United States or such other locations described in a Quote or other documentation from us to you; however, we may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes. Should it be necessary to do so, you and we will review supplemental measures that may be required based on applicable Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of protection. Under those circumstances, you and we agree to work together in good faith to find a mutually acceptable resolution to address such supplementary measures.

Security; Confidentiality

We will maintain appropriate technical and organizational security measures for the Processing of Personal Information in our possession or control designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. Our security measures may include, for example, (i) utilizing firewall, router, and VPN-based access controls, (ii) regular examinations of security risks, (iii) role-based access controls implemented in a manner consistent with the principle of "least privilege," (iv) logging of all access to host servers, applications, databases, routers, switches, etc., (v) password protection that includes minimum length requirements and periodic resets, (vi) implementation of anti-malware and anti-spyware solutions, and (vii) security incident and event

management (SIEM) systems. All ICS and ICS Affiliates employees, and Third-Party Subprocessors that Process Personal Information, are subject to written confidentiality arrangements.

Audit Rights

Timing: You may audit our compliance with our obligations under this DPP up to one time per year at your cost. More frequent audits will be permitted if expressly required by Applicable Data Protection Law.

Requests: We must receive your request for an audit in writing and no less than two (2) weeks before the proposed audit date. Your request must describe the proposed scope, duration, and start date of the audit. We will promptly review the proposed audit plan and provide you with any concerns or questions, and work cooperatively with you to agree on a final audit plan within a reasonable timeframe. Audits must be conducted during regular business hours and may not unreasonably interfere with our normal business activities.

Third-Party Auditors: If you engage a third-party auditor to conduct an audit, the third-party must be mutually agreed to by you and by us unless the third-party is a Regulator. We will not unreasonably withhold our consent to a third-party auditor; however, prior to conducting any audit, a third-party auditor must execute a written confidentiality agreement reasonably acceptable to us or otherwise be bound by a statutory or legal confidentiality obligation.

Copies: You agree to promptly provide us with a copy of any audit report, which will be considered confidential information. You agree to use or disclose the audit report only for the purposes of meeting your regulatory audit requirements and/or confirming compliance with the requirements of this DPP, and for no other purpose. Each party will bear its own costs in relation to the audit, unless we promptly inform you upon our review of the audit plan that we expect to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under the Services Agreement, such as additional license or third-party contractor fees. You will be responsible for paying those fees; however, we agree to try in good faith to mitigate those fees to an extent reasonably practicable.

Acceptance of Prior Reports. Notwithstanding the foregoing, if the scope of a proposed audit is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or a similar audit report issued by a qualified third-party auditor within the prior twelve (12) months from the date of your audit request, and if we provide that report to you confirming there are no known material changes in the controls audited, you agree to accept the findings of the report in lieu of an audit of the same controls covered by the report.

Incident Management and Breach Notification

If we confirm that an Information Breach has, or likely has, occurred, then we will notify you the situation without undue delay but at the latest within 72 hours after confirmation. As information regarding the Information Breach is collected or otherwise becomes available to us, we will also provide you with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with us on the content and timing of any public statements or required notices to affected Individuals and/or notices to relevant Regulators.

Return and Deletion of Personal Information

Upon termination of the Services, we will either promptly return or destroy (at our discretion) the Personal Information in our custody or control; provided, however, we shall be entitled to retain a copy of part or all of the Personal Information

as reasonably necessary to evidence the parties' business relationship and/or the scope or type of Services provided or facilitated thereunder. Any Personal Information retained shall be considered to be your confidential information, and shall be treated as such at all times.

Legal Requirements

If we are required by law to provide access to Personal Information (such as to comply with a subpoena or other legal process, or to respond to government requests), then we will promptly inform you of that requirement. If, in the opinion of our counsel, a request for access ("Access Request") is legally valid and binding on us, then we will provide access as required unless we are otherwise ordered by a court of competent jurisdiction to refrain from doing so. You agree to indemnify us for all fees, costs, and expenses we incur in the process of determining whether the Access Request is valid, as well as any subsequent fees and costs we may incur relevant to the disclosure process.

Data Protection Officer

ICS's Chief Privacy Officer and local Data Protection Officer is Melanie Agee, email: magee@chooseics.com.

Definitions

- "**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this DPP, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended ("CCPA") and other U.S. state laws.
- "**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.
- "**Applicable UK Data Protection Law**" means (i) the UK GDPR, meaning the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020; and (ii) the UK Data Protection Act 2018, as amended.
- "**Europe**" means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.
- "**Individual**" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.
- "**Information Breach**" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed on systems controlled by ICS.
- "**Master Services Agreement**" means the master terms and conditions applicable to all services provided or facilitated by ICS, a copy of which can be found at https://www.chooseics.com/msa.
- **"Process/Processing", "Controller", "Processor"** and **"Binding Corporate Rules"** (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.
- "**Quote**" shall have the meaning set forth in the Master Services Agreement.

- "**Service Provider**", "**Sell**", "**Share**", "**Business Purpose**", and "**Commercial Purpose**" have the meaning set forth under the law of the state in which you are headquartered; however, if no such law reasonably applies or defines such terms, then the terms shall have the same meaning as indicated in the CCPA.
- "**ICS Affiliate(s)**" means the subsidiar(y)(ies) of ICS that may Process Personal Information as set forth in this DPP.
- "**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.
- "**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.
- "**Services**" or the equivalent terms "**Service Offerings**" or "**services**" means any services that you have purchased through one or more Quotes.
- "**Third-Party Subprocessor**" means a third-party, other than a ICS Affiliate, which ICS subcontracts with and which may Process Personal Information as set forth in this DPP.

List of Approved ICS Subprocessors

Note: Subprocessors may have their own list of subprocessors. Please see each subprocessor's site for details.

Entity Name	Processing Activity	Location
Acronis	Backup, Disaster Recovery, Cloud Storage	USA
Atakama	DNS/Browser Filtering	USA
Blumira	Security Monitoring (SIEM), Log Collection, Threat Detection	USA
Cynomi	vCISO Platform, Security Assessments, Risk Management	USA
DocuSign	Electronic Signature	USA
Fireflies.ai	AI Meeting Transcription, Recording & Note Processing	USA
GoDaddy	Domain Registration, DNS, Website Hosting	USA
IRONSCALES	Email Security, Anti-Phishing, Threat Detection	USA
Keeper	Password/Identity Management	USA
Liongard	Dark Web Monitoring, Change Management	USA
Microsoft	Microsoft 365, Dynamics, Email, File Storage, Identity Services	USA
Petra	ITDR	USA
Proofpoint	Email Security, Spam Filtering, Email Encryption	USA
SentinelOne	Endpoint Protection, Threat Detection & Response	USA,
Syncro	PSA, RMM, Remote Monitoring, Ticketing	USA

Last Updated: July 2026