
Service Level Agreement (SLA)

Updated: April 30, 2023

Effective: May 1, 2023

This Service Level Agreement (the "SLA" or the "Agreement") sets forth the terms and conditions that govern the work performed by Great River Strategies (the "Provider") for its clients who both have and do not have contracts (the "Client").

1. **Definitions.**

- a. "Client Onboarding" is the 30-day period of time used to collect information, observation, documentation, and share process-related logistics between the Provider and Client. The 30-day period begins upon signature of both parties on a Technology Consulting Agreement.
- b. "Confidential Information" means all information disclosed by the Client to the Provider electronically, visually, orally, or in a tangible form which is either marked as "confidential" or with a similar legend or is identified at the time of disclosure as being confidential, information pertaining to the Client donor names and giving records, personnel files, personal documents, ePHI, and financial records, business plans and processes, and all information generally considered to be confidential or should be reasonably understood to be confidential or proprietary. Confidential Information can also include access information or account credentials, such as usernames and passwords.
- c. "Resolve" or "Resolution" of an issue or issues means a solution the Provider presents and, in the Provider's best judgment, is a workable fix to a Client request, such as a technical issue or problem.
- d. "Response" is defined as any form of reply or action, observable or unobservable to the Client, taken by the Provider in an attempt to resolve a Support Request from the Client.
- e. "Service" or "Services" includes any and all professional technology or other consulting services, including but not limited to the following examples, in the area of "IT Help Desk" and "IT Support", including, general desktop technology support, mobile device support, routine network & system monitoring, computer software support, computer hardware support; "IT Project" and "IT Consulting" and "Consulting", including, server & e-mail conversion, technology policy support, CTO services, computer network support, RFP consulting services, or software selection guidance; "Routine Security & Stability Maintenance", including, back-end security and systems management; and other technology or system process support needs as outlined in this Agreement.
- f. "Service Request" and "Ticket" and "Support Request" and "Request" means a formal request initiated by the Client to the Provider requesting support, counsel, advice, or consulting regarding Services, which are billable under this Agreement. The Provider may or may not consider any call, email, text, or other request made to an agent of the Provider to be the activation of a Ticket based on the Provider's professional judgment.
- g. "Technology Resource(s)" means any computers, workstations, laptops, tablets, phones, servers, switches, modems, routers, and/or any other hardware, software (local, hosted, or cloud-based), accounts, and technology equipment, tools, or accessories.
- h. "Third Party" hardware, software, or other technology resource or Managed Resource that is owned, controlled, managed, rented, or otherwise falls under or depends on, either partially or wholly, a separate company, organization, or individual apart from the Client and Provider.

- i. “Your Data” or “Client Data” means any information stored on electronic equipment including computers hard drives, whether on site, off site, or in a remote (i.e. cloud) location, and other information or knowledge, resources, applications, or data that is owned or retained by the Client.

2. Services.

- a. The Provider categorizes Services under several categories in an effort to provide greater understanding of Service delivery, issue tracking and cataloging, and technology planning. The most common Service categories are: IT Help Desk, IT Support, IT Project, Routine Security & Stability Maintenance, IT Consulting, and Project Consulting.
- b. All examples listed under Service categories are for illustrative purposes only and are not intended to constitute a complete list or exact definition under each category. Every Service Request is unique and based on the specific details of an individual Service Request. Provider has the sole discretion regarding the Service categorization.
- c. Maintenance or repair of some problems (e.g., software glitches, poor hardware design), and with Third Party software and hardware, depends on that Third Party’s initiative or response to that particular problem. The Provider is not responsible for and cannot directly fix these issues, though the Provider will assist in finding work-around solutions for these problems as available and following Third Party agreements.
- d. **Technology Managed Services.** Services that fall under Technology Managed Services may cover some or all Services or Service categories for a set monthly fee rather than the Provider billing per hour of Services delivered on Managed Resources. The Terms and Services and the applicable Agreement with the Client will specify which Services are covered under Technology Managed Services.
- e. **Technology Co-Managed Services.** Services that fall under Technology Co-Managed Services may cover some or all Services or Service categories for a set monthly fee rather than the Provider billing per hour of Services delivered on Co-Managed Resources. The Terms and Services and the applicable Agreement with the Client will specify which Services are covered under Technology Co-Managed Services.
- f. **IT Help Desk.** Services that fall under IT Help Desk are often unplanned, spontaneous, or urgent Support Requests that generally involve a current impact on the Client’s uptime or productivity and therefore require a time-sensitive resolution.
 - i. IT Help Desk requests are spontaneous or unplanned and usually initiated by the Client or one of the Client’s automated systems, such as downtime or email breach monitors that send automated notifications to the Provider. The Provider typically does not have foreknowledge of the request and did not account for the request in the Provider’s schedule or calendar ahead of time.
 - ii. IT Help Desk requests are treated as time-sensitive by the Provider, but it is the responsibility of the Client to define and outline during the initial request the time-sensitive nature of the request.
 - iii. The Provider may separate or divide a single Service Request across multiple Service categories, including having a Service Request fall under IT Help Desk and overlapping with IT Support.
- g. **IT Support.** Services that fall under IT Support involve Support Requests made by the Client or involve Services initiated by the Provider on behalf of the Client. IT Support is the most general and common Service category.
 - i. IT Support includes fixes and repairs for a technical problem on a Managed Resource to restore it to or maintain a functioning state.
 - 1. Examples of this may include addressing errors, malware, inability to log in, restoration from data backup, recovery of hardware failure, networking problems, system access problems, etc.
 - ii. IT Support includes the replacement of Managed Resource hardware and local-user software.
 - 1. This refers to labor by the Provider in which an existing Managed Resource is no longer functioning as intended and an equivalent (or modern equivalent) piece of hardware or software is being implemented in its place.

2. Some common examples of scenarios that require a replacement:
 - a. The emergence of an unfixable malfunction or corruption: a device or application is beyond the point of “fixability” via any feasible repair measure.
 - b. Performance has declined over time to the point of being impractical to use.
 - c. Approaching or having just passed the end of the hardware manufacturer’s or software developer’s support scope, which is often indicated via an “end of life” (EOL) date published by the third-party vendor.
3. Some noteworthy examples of scenarios that are NOT considered to be a replacement but would instead be considered an IT Project:
 - a. The new deployment is not replacing an existing hardware or software. The most common example of this is a deployment for a newly created staff position.
 - b. An existing hardware or software is functioning as expected, but the Client requests to implement something in its place that’s of a higher grade or that has a different set of capabilities to the existing Resource.
- iii. IT Support includes routine user account management and license management of an existing software system; including but not limited to the creation of, deletion of, archiving of, and other related common account modifications for user accounts.
- h. **IT Project.** The Provider offers IT Project Services that involve any technology project that adds to, expands upon, upgrades, or significantly changes the Client’s existing technology landscape, which includes the Client’s Managed Resources, covered set of hardware, software, cloud services, features, functionalities, networking systems, or tech-related service providers.
 - i. IT Project Services may be a request initiated first by the Client, or by the Provider with consent of the Client.
 - ii. IT Project Services often fit a specifically defined project that may or may not overlap or interact with the Client’s regular business operations or technology infrastructure. The Provider determines when an IT Project reaches the scope that warrants the design, scheduling, and outlining of a project plan.
 - iii. The Provider attempts, when possible, and often when projects require extended hours or coordination between Provider staff, to provide an outline scope of IT Project Services that can easily be categorized under one project, or multiple projects as needed, including a list of IT Project Services provided and projected budget and timeline.
 1. Budget and timeline projections, and technical recommendations, are based on information disclosed and collected from the Client, and are based on the Client’s feedback regarding priority, strategy, and organizational workflow. These are merely an estimate, and are subject to change, and should not be considered a purchase order or formal quote of any kind.
 2. While the Provider makes every attempt to outline a project plan, the Client understands an IT Project may involve unforeseen items, complications, IT Support Requests, and other billable items not explicitly outlined in an IT Project plan, estimate, or proposal. As projects nearly always require coordination between Client and Provider staff, the Provider does not guarantee timelines or budgets for IT Project Service.
- i. **Routine Security & Stability Maintenance.** Services that fall under regular, scheduled hardware or software maintenance and updates in accordance with Provider best-practices, performed for the relevant existing Managed Resources according to and prompted by the Provider set maintenance schedule.
 - i. Routine Security & Stability Maintenance Services only apply to maintenance and updates performed as part of the Provider’s maintenance scheduled routines. This category does not include ad hoc requests from Client, or Client-initiated maintenance Services, regardless of whether it relates to what may be considered standard maintenance or security updates.

STRATEGIES

- j. **IT Consulting.** Services that fall under IT Consulting often fit high-level technology planning, strategy, development, or unique or specific technology system design, integration mapping, or system development.
 - i. IT Consulting Service may include custom recommendations regarding which or whether upgrades to Managed Resources would be fitting for the Client.
 - ii. IT Consulting Service may include the guidance on how to select which Managed Resource to purchase or migrate into or strategize regarding how best to manage the commissioning or decommissioning of users, equipment, software, hardware, or other Managed Resources.
 - iii. Staff training, group training, or individual training or counsel regarding Managed Resource utilization may fall under IT Consulting Service.
- k. **Project Consulting.** Services that fall under Project Consulting are typically high-level strategic counsel, consulting, or project management for impact system changes. The Services may involve consultation over multiple months as part of a strategic project plan.
 - i. Examples of this may include:
 - 1. The selection of a new electronic health resource system (EHR).
 - 2. Determination, vetting, and selection of a new database tool, system, or application development.
- l. **Miscellaneous Services.** Services that fall under Miscellaneous Services are not easily defined or do not readily fit into other Service categories. Services delivered that do not fit other Service categories may fall under this category as determined appropriate by the Provider.
- m. **Not Managed Resource Support.** Services that fall under Not Managed Resource Support are for Service delivery on any hardware, software, tool, equipment, or other technology resource that is not managed by the Provider. The Provider, in collaboration with the Client, maintains a complete list of Managed Resources and uses the Client "IT Database" to determine whether Services fall under Not Managed Resource Support.
 - i. Not Managed Resource Support may include Technology Resources that had previously been managed or otherwise supported by the Provider, for example, but not limited to, aging hardware or out-of-date software, but the Technology Resource no longer meets the criteria to receive Managed Resource Support, or security risks deem the Technology Resource too great of a liability.
 - ii. Based on a manufacturer, developer, or other third-party recommendation, expiration date, end of support, best practices, or solely based on the professional judgment or the performance of a Technology Resource, the Provider may change the status of any Technology Resource(s) from Managed Resource(s) to be listed and fully considered a Not Managed Resource(s) at any time without prior approval of the Client and therefore that Technology Resource(s) would be subject to any and all Not Managed Resource Support Service.
 - iii. The Provider will make reasonable efforts to notify the Client whenever a particular resource transitions from "managed" to "not managed" status. When possible, this notice will be given ahead of the transition of status.
- n. **Emergency IT Service.** Services that fall under Emergency IT Service are spontaneous, time-sensitive, or fall outside of the Provider's business hours as outlined in this SLA. Emergency IT Service also applies for all hours, time, and effort spent identifying, recovering, resolving, and remediation for any cybersecurity incident, security breach, data loss, or other incident or incidents occurring as a result of Client not following Provider's security improvements, recommendations, projects, or other guidance presented as recommended or necessary security measures or improvements.
 - i. Emergency IT Service applies for Service Requests made outside of Provider business hours or closure dates due to holidays or other events.

STRATEGIES

- ii. For Emergency IT Service after hours, during weekend days (Saturday, Sunday, and Monday), the Client must contact the Provider via phone, voice message, or text to: (612) 412-4606 and include the word “emergency” or “urgent”. Failure to include either of these words may result in a delay of Emergency IT Service until the Help Desk opens the next business day.
- iii. Emergency IT Service may apply during Provider business hours if the Client Service Request requires a resolution more urgently than the response time outlined in this SLA.
- iv. Emergency IT Service may apply under a technology project as defined under “IT Project” or “IT Consulting” if and when the Client requests an accelerated project timeline. This can include, but is not limited to, the Client requesting a new or previously discussed IT Project be completed sooner than the Provider schedule has normal capacity to deliver. The determination of when Emergency IT Service applies under a project schedule is at the discretion of the Provider. Requesting an accelerated timeline resulting in the need for Emergency IT Service negates previously quoted hours and rates, including a flat rate project quote.
- v. In the event of the discovery of a suspected security breach, data breach, or other security breach as determined by the Provider, the Provider may act on taking reasonable steps to address the security breach without direct consent from the Client in an effort to more quickly resolve any issues or limit the Client’s exposure.

3. Provider Business Hours & Closures.

- a. Business hours are defined as Monday, Tuesday, Wednesday, Thursday and Friday, 8 a.m. – 5 p.m. CT.
 - i. During weekends (Saturday and Sunday) response time is eight hours from the start (8 a.m.) of the next business day (Monday-Friday).
 - ii. The Provider may be closed, Service may be delayed, or business hours may be adjusted for the following holidays or events: Martin Luther King Jr.’s Day, President’s Day, Good Friday through the Monday after Easter, Friday before Memorial Day through Memorial Day, Juneteenth, July 3 through July 5, Friday before Labor Day through Labor Day, Veterans Day, Wednesday before Thanksgiving through the Monday after Thanksgiving, Christmas Eve Day through January 2nd. The Provider may match the Federal Holiday schedule for Federal Holiday Observed dates. Provider will respond to support requests within 24 hours of the next business day that the Provider is open.
 - iii. Events out of the Provider’s control, such as extreme weather, power outages, internet services provider outages, acts of God, pandemic events or other localized health events, and other events that may impact Provider staff or staffing levels may result in a delay of Service.
 - iv. Requests made outside of business hours or requiring the Provider to provide Service outside of business hours or urgently or immediately during business hours, may fall under “Emergency IT Services” and may be billed as such.

4. Services Delivery.

- a. Service Delivery or response time does not apply to Project Consulting Services due to the complex nature of this service.
- b. Upon receiving a Service Request, a Ticket will be created and assigned to a Provider agent within two business days of initial contact from the Client as outlined under Service Request Initiation.
- c. A Resolution shall be presented within two business days of the creation of a Ticket, subject to Provider Business Hours & Closures.
- d. Resolutions may be delayed without notice to the Client in the following cases (not an exhaustive list):

- iv. Support representative(s) cannot procure further needed information regarding the nature and symptoms of the problem, including delayed responses from the Client or a Client representative.
- v. The Provider's Resolution includes or otherwise depends upon the response time of a Third Party.
- vi. The Provider's workload is unusually high.
- vii. The particular problem features special complexity or complications.
- viii. The request is attached to a Project Consulting agreement to select an application, software, or tool, and response time requires additional thought, processing, research, or consideration.
- e. Resolution efforts may be abandoned in the following cases (not an exhaustive list):
 - ix. A problem cannot be reproduced using similar hardware or software configuration.
 - x. The Client or Client representative cannot give enough information required to resolve the problem.
 - xi. The Resolution requires custom improvements or unplanned updates.
 - xii. A user carries out actions that break end user license agreements or technical requirements for installation and use of any Third Party products; or the Client exceeds the allowed number of software installations.
 - xiii. The Client has been shown to be in possession of or usage of unlicensed or illegal software.
 - xiv. The question is beyond the Provider's scope of Service.
 - xv. The Client or a Client representative is nonresponsive or unable to effectively communicate the issue.
 - xvi. The Service delivery or Resolution may be impacted by Federal, State, or other local government restrictions, or internal Client or Provider policies, for example, but not limited to, pandemic response plans, such as COVID-19 closures and restrictions or vaccination policies. The Provider retains absolute discretion regarding staff onsite visits and may limit or abandon Service delivery if the Provider determines the onsite Resolution would result in potentially negative health impacts on Provider staff member(s) or violate the Provider's internal policies.

5. Client Obligations.

- a. The Client has access to the "IT Database" maintained by the Provider. The Client acknowledges the IT Database is the sole system used to list all proposed Managed Resources and the Client has comment privileges to the IT Database. The Client is responsible to fully review and recommend any changes, additions, or subtractions within the Client Onboarding period and any and all items not listed fall outside the Managed Resources and scope of this SLA, and outside the obligations and are unknown to the Provider.
- b. The Client understands and agrees to restrict and manage internal access to Confidential Information, including limiting and restricting access to the IT Database and access credentials. The Client establishes who has access to information and is responsible for communicating these restrictions with the Provider.
- c. The Client agrees to notify the Provider in advance of adding or removing any technology, whether hardware, software, or accessory, that interacts with the Client's technology system, infrastructure, or Managed Resources falling under this SLA. The Client understands the Provider does not or may not support resources not disclosed to, or documented by, the Provider. The Client acknowledges the Provider is not responsible for issues that may result or may have resulted from a Not Managed Resource.
- d. While the Provider may ask and make assumptions of a Service Request's priority, it is the sole responsibility of the Client to indicate the priority level of a Support Request.
- e. The Client is responsible for understanding agreements made with software, hardware, software-as-a-service (SAAS), and hosting providers, and any other second or Third Party providers. The Provider may offer counsel regarding how to interpret such agreements, but does not accept ownership for understanding, delivery, resolution, or fulfillment of second or Third Party agreements, including, but not limited to, data backup services, data recovery services, printer and copier services, internet service provider services, and software agreements, including up-time, the scope of development needs, and customization requirements.

STRATEGIES

- f. The Client understands that the Provider has the right to determine the expiration date of a managed resource due to the vendor or manufacturer's guidance on firmware, system support, update guidance, and other conditions placed on Technology Resources that are outside the control of the Provider. The Client or the Provider may request an annual meeting to review and suggest changes to the IT Database.
- g. The Client understands the ongoing maintenance, including system security, is the Client's sole responsibility to initiate in partnership with the Provider. While the Provider may consult what may be considered recommended, essential, standard, or required system updates, patches, and upgrades, the Client is responsible for requesting and pre-approving in writing that this work be performed by Provider. The Provider does not accept liability for incidents or actions that were a result of a system, software, or any Technology Resources that were not maintained or updated as recommended by the Technology Resource vendor.
- h. The Client is responsible for providing reasonable advance notice to the Provider for any change, adjustment, or discontinuation of Third Party service(s) such as, but not limited to, internet service provider ("ISP") change, phone service provider modification, accounting software change, and copier service provider adjustments, that have an impact on Technology Resources. Reasonable advance notice is defined as a minimum of 30-calendar-days, but preferably several months or more based on the impact of a service change on the Client's internal operations or functionality, which can only be initiated and initially determined by the Client. Failure to provide such advanced notification may result in serious Service interruption or loss of critical functionality.
- i. The Client is solely responsible for the physical security of all Client-owned or leased Technology Resources, including, but not limited to, workstation computers, laptops, tablets, phones, servers, networking equipment, and other devices, components, or other Technology Resources. The Provider may offer specific advice regarding securing Technology Resources, but it is the responsibility of the Client to implement these security measures. The Client is responsible for the physical security of their building, site, or location. The Client is responsible for making additional physical security improvements based on situations or circumstances.

6. **Confidentiality.**

In the course of performing Services, the parties recognize that the Provider may come in contact with or become familiar with Confidential Information. The Client is responsible for defining and documenting in writing a complete description or list of Confidential Information. The Provider agrees to keep all such Confidential Information confidential and not to discuss or divulge it to anyone other than appropriate internal Client personnel and authorized Provider staff who need to know such Confidential Information. The Client agrees and understands that confidentiality may be waived without notice to comply with certain State and Federal laws, such as laws regarding the discovery of suspected criminal acts such as, but not limited to, child pornography, and if discovered may be reported to appropriate law enforcement agencies.

The Provider acknowledges that all Confidential Information disclosed by the Client to Provider for the purposes of performing its obligations under this Agreement constitutes a valuable asset of, and is proprietary to the Client. The Provider also acknowledges that the Client has a responsibility to its employees to keep their records strictly confidential. The Provider shall not disclose the Confidential Information or knowingly permit its employees, officers, agents, or contractors to disclose such Confidential Information to any person outside of Provider, or to any person within its company not having a specific "need to know" in performance of their work in connection with the Services provided to the Client hereunder. The Provider shall take reasonable steps to ensure fulfillment of this obligation, including instructing its employees and contractors not to sell, lease, assign, transfer, or reveal any Confidential Information without the Client's prior consent.

In the event that a subpoena or other legal process in any way concerning information disclosed by the Client to the Provider is served upon the Provider, the Provider agrees to notify the Client reasonably upon receipt of such subpoena or other legal process unless otherwise provided by law and to cooperate with the Client, at the Client's

expense, in any lawful effort by the Client's contest the legal validity of such subpoena or other legal process, provided nothing herein shall be interpreted to mean that the Provider will not comply with any lawful requirement of any federal or state court or agency with respect to disclosure of Confidential Information of the Client. In addition, this provision will in no way limit the Provider's ability to satisfy any governmentally required disclosure of its relationship with, or Confidential Information of the Client. The data or information held by, or maintained by, the Provider, will be made available for inspection by the Client's supervisory authorities, or, if authorized by the Client in writing, or other designated person(s). The Provider's obligations under this Section are subject to and limited by the any provisions of the applicable Agreement regarding termination which may allow the Provider to dispose of materials and/or Confidential Information of the Client upon termination of the Agreement.

7. Changes to this SLA.

The Provider may revise this SLA from time to time. The most current version of the SLA will govern the Service delivery and work between the Provider and Client and will always be at <https://www.greatriverstrategies.com/sla>. If the Provider makes a change to this SLA that, in the Provider's sole discretion, is material, the Provider will notify the Client via an email to the Client's primary business contact email address on file with the Provider. By continuing to access or use Services after those changes become effective, the Client agrees to be bound by the revised SLA.

8. Notice.

Any notice or communication permitted or required by this SLA to the Provider, beyond that of Services, shall be permitted through email directly to the Provider primary business contact, Joel Barker, joel@greatriverstrategies.com or first-class mail to Great River Strategies, Attn: Joel Barker, 5115 Excelsior Blvd Ste 713, Minneapolis, MN 55416.

9. Warranties and Disclaimer.

- a. All Services will be performed in a professional manner in accordance with industry standards. If a Service has been improperly performed, the Client must notify the Provider in writing within thirty (30) days of the occurrence of the problem, and the Provider will reperform the Service at no charge, if requested. The foregoing provides the Client the sole remedy for Resolution for Services that do not comply with the Section 10.
- b. Client Warranties: Client represents and warrants that (a) its Client Data and any other materials or information provided by Client to the Provider in connection with this Agreement will not violate any person's right of privacy or any third party copyright, trademark, or other intellectual property rights, and that Client and its Authorized Users will not transmit any such materials to Provider; and (b) Client and its Authorized Users will use the Services only as permitted by law and regulation.

- c. PROVIDER EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY (BY ANY TERRITORY OR JURISDICTION) TO THE EXTENT PERMITTED BY LAW, ANY WARRANTY OF NON-INFRINGEMENT, TITLE, FITNESS FOR A PARTICULAR PURPOSE, OR MERCHANTABILITY. PROVIDER WILL NOT BE LIABLE TO CLIENT FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE OR SPECIAL DAMAGES, OR FOR ANY LOSS OF PROFIT (WHETHER DIRECT, INDIRECT OR CONSEQUENTIAL), REGARDLESS OF THE FORM OF THE ACTION OR THE THEORY OF RECOVERY, EVEN IF CLIENT HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES. THE PROVIDER SHALL NOT BE LIABLE TO THE CLIENT OR ANY THIRD PARTIES FOR THE ACTS OR OMISSIONS OF THE PROVIDER PURSUANT TO THIS SLA. THE PROVIDER DOES NOT GUARANTEE RESULTS, INCLUDED BUT NOT LIMITED TO, IT SUPPORT SERVICE RESULTS, NETWORK "UP TIME", FILE, NETWORK, OR INFORMATION SECURITY, HIPAA COMPLIANCE, PCI COMPLIANCE, CLIENT INDUSTRY TECHNOLOGY REQUIREMENTS, RESTORATION OF ANY DATA, INCLUDING BACKED UP DATA, VERIFICATION OF DATA BACKUP SYSTEM(S), PROTECTIONS FROM RANSOMWARE, VIRUSES, OR MALICIOUS SOFTWARE, OR RESULTS REGARDING THIRD-PARTY HARDWARE, THIRD-PARTY SOFTWARE, OR ONLINE TOOLS. THE TOTAL LIABILITY OF PROVIDER UNDER THIS AGREEMENT FOR ANY CAUSE SHALL NOT EXCEED (EITHER FOR ANY SINGLE LOSS OR ALL LOSSES IN THE AGGREGATE) THE TOTAL AMOUNT PAID UNDER THIS AGREEMENT BY CLIENT FOR THE PREVIOUS ONE (1) MONTH.

10. **Client Data.**

The Client owns the Client data, and all Confidential Information and any user data, access information, including passwords, and other electronic data that the Client may provide to the Provider ("Your Data"). In order for the Provider to deliver Services, the Client grants to the Provider and its contractor's permission or a license to use, reproduce, store, and modify Client Data for the sole and exclusive purposes of providing Services to or on behalf of the Client.

The Provider acknowledges that the Client owns the information contained within the IT Database. Upon formal, authorized, and verified request from the Client, the Provider will provide complete access to and export of all information contained within the IT Database.

The Provider takes the privacy and security of the Client's Data seriously. The Client is responsible for establishing internal policies and procedures for limiting the disclosure of, or access to, all data, including sensitive, private, or confidential data. The Client is also responsible for sharing policies and procedures, including any updates or changes, with the Provider. The Provider has established internal policies and procedures for data disclosure that may support the protection of some data, however, it is the sole responsibility of the Client to adopt these policies and procedures, or to determine how they may fit within or contradict internal Client policies and procedures. The Client assumes all responsibility for updating and changing authorization as necessary.

The Client is responsible for establishing internal policies and procedures for limiting the disclosure of, or access to, all data, including sensitive, private, or confidential data. The Client is also responsible for sharing policies and procedures, including any updates or changes, with the Provider. The Provider has established internal policies and procedures for data disclosure that may support the protection of some data, however, it is the sole responsibility of the Client to adopt these policies and procedures, or to determine how they may fit within or contradict internal Client policies and procedures. The Client assumes all responsibility for updating and changing authorization as necessary.

11. **Policy and Documentation Management.**

The Client is solely responsible for the approval, or non-approval, implementation, management, dissemination, and training regarding Client policies. The Provider may support or provide as a Service the development, consulting, advising, or drafting of policy documents for general or specific use by the Client; however, the final determination, language, and effectiveness of policies is solely at the discretion of the Client. The information, templates, forms, tips, and tools provided by and through the Provider or representatives of the Provider are not legal advice. The Provider is not a law firm. The Provider's employees, contractors, and representatives are not attorneys. The employees and contractors (including attorneys, if any,) of the Provider are not acting as the Client's attorneys, and none of them are a substitute for the advice of your own attorney or law firm licensed to practice law in your state. The employees or contractors of the Provider who wrote or modified any policy document, form, template, tip, or tool are NOT providing legal advice or legal counsel, and are not creating or entering into an Attorney-Client relationship. The Provider will take every reasonable effort to attempt to make sure information, documents, and templates are accurate, up-to-date, and useful, the Client understands they should consult an attorney licensed to practice law in their state to receive professional assurance that any and all materials, documents, templates, and the Client's interpretation of it or them, and the information and input that the Provider or Client provides, is appropriate to the Client's particular situation. Provider-created documents, templates, tools, and information are not guaranteed to be correct, complete, or up-to-date.

12. Advice Disclaimer and Reporting.

The Provider's tools and templates where Client provides information or makes choices, even if based upon suggestions or tips provided by the Provider, and resulting in a document where that information or the outcome of Client's choices, does not and is not intended to represent the advice of the Provider, or the practice of law. The Provider is not permitted to engage in the practice of law. The Provider is prohibited from providing any kind of advice, explanation, opinion, or recommendation to a consumer about possible legal rights, remedies, defenses, options, selection, or completion of forms or strategies.

The Provider may create, generate, or otherwise produce Service reports or documents that illustrate Service delivery. Reports illustrating confidence ratings or percentages are for illustrative purposes only and do not represent a guarantee.

INFORMATION IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF INTELLECTUAL PROPERTY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT SHALL GREAT RIVER STRATEGIES, OR ITS AGENTS, SHAREHOLDERS, OFFICERS OR ATTORNEYS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, LOSS OF DATA OR ACCESS TO DATA) ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION, EVEN IF Great River Strategies HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Communications between you and the Provider are protected by the Provider's Privacy Policy (<https://www.greatriverstrategies.com/privacy>). Please also note that your relationship with the Provider is subject to additional terms of service.

The Provider does not provide legal guidance, the Client must determine the response necessary based on the advice of their legal counsel and internal policies, contracts, regulations, and local, state, and federal laws.

13. Data Breach or Loss of Your Data.

The Client understands the Provider does not directly host the Client's data. The Provider will make every attempt to counsel and advise the Client regarding data maintenance, continuity, data backup, and security measures and recommendations. The Provider is not responsible for the actions or inactions of the data host selected by the Provider, or Client decisions that may result or may have resulted in the loss of data or loss of access to data or other Managed Resources or technology resources, such as database base systems. The Client is solely responsible to develop and maintain a data retention system, process, and policy that matches any and all legal, industry specific compliance needs, or any business or other needs or requirements. The Provider does not monitor, regulate, or otherwise manage the Client's data, including the data retained by individual Client employees, leaders, owners, contractors, or any and all other parties that may have access to the Client's data.

14. **Software and Hardware.**

The Provider is not a vendor or reseller of software, hardware, or technology resources. Through the course of providing Services, the Provider may make recommendations or provide counsel or direct consultation Services regarding the selection of software, hardware, or other technology Managed Resources. The Provider is not responsible for the impact of the selected software, hardware, or other technology Managed Resource. The Client owns all software, hardware, and other technology Managed Resources and should review and understand all risks, warranties, disclosures, or other disclaimers provided by or available through the software, hardware, or retail vendor.

The Provider will select a Third Party software tool or tools for use with providing Services. The selected software tool(s) will be from a reputable source meeting industry standards and best practices as vetted and determined by the Provider. The Client agrees the Provider is permitted to select the software tool(s) at the Provider's sole discretion, and the Client permits the Provider to install this software on Client Managed Resources for the purpose of delivering Services. The Client understands the Provider is not liable or responsible for any negative impact as a result of the software, including downtime, security breaches, or negative impact on Provider Service delivery.

- a. The Provider has the sole discretion to select approved software applications or tools which may be referred to collectively as "Support Tools" or "RMM Software + Security and Documentation Tools" for remote connectivity or access, such as virtual private network ("VPN"), remote desktop connection ("RDC"), remote monitoring and management ("RMM"), or other remote connectivity. The Provider may reject, uninstall, and deny access without notice to software, applications, or other tools determined to be a security threat, vulnerable to security threats or misuse, or otherwise unnecessary or counter-productive to the Provider or the Provider approved software application(s).
 - a. The Provider has approved the following RMM Software + Security and Documentation Tools
 - i. [NinjaOne RMM](#)
 - ii. [IT Glue \(a Kasaya Company\)](#)
 - iii. [HaloPSA](#)
 - iv. [Senserva](#)
 - v. [Google Workspace](#)
 - vi. [TeamViewer](#)
 - vii. [AnyDesk](#)
 - viii. [Dropbox](#)
 - ix. [Privnote](#)
 - x. [uSecure](#)

- b. The Provider is responsible to monitor all security notices released by the selected Third Party, RMM, and make or reject any security updates or patches based on the most recent releases. The Provider reserves the right to change Third Party “RMM” vendors at any time and without notice for valid cybersecurity reasons based on published security notices or security recommendations from reputable sources as determined by the Provider.
- c. The Provider may require the Client to designate or purchase a computer, commonly referred to by the Provider as a “System Management PC” for the purpose of Service delivery, such as remote monitoring and system administration. The Provider reserves the sole right to select a computer that will meet the Provider’s Service requirements. The Client retains ownership of the computer hardware and the Provider retains full administrative privileges to the “System Management PC” for the duration of this Agreement. As determined necessary by the Provider, the Client may be required to purchase additional “System Management PC” computers for each Client site, location, or building, and as needed, the Client may be required to purchase replacement “System Management PC” computers

15. **Security and Cybersecurity.**

The Provider may consult and advise the Client regarding information and technology security and cybersecurity, including network security, workstation security, mobile device security, security policies, and other information and technology security topics and issues. The Client understands the Provider does not directly provide software tools or other tools that provide system security. The Provider is not responsible for the actions or inactions that result in a security breach. Upon request from the Client, the Provider may consult regarding security policies, best practices, and security software selection. The Provider is not responsible for the implementation of security policies, procedures, security software, and security hardware. The Provider is not responsible for the Client sustaining a security breach, including but not limited to ransomware, hacking, or otherwise unauthorized access or malicious activities in the Client’s data or systems.

The Client understands that Confidential Information may be retained within the Provider’s secure documentation system. The Provider agrees to maintain this information in a secure environment.

A Client receiving Technology Managed Services or Technology Co-Managed Services is required to have a Provider approved Multiple Factor Authentication (“MFA”) structure in place for all accounts, services, and systems where MFA is available. The Provider reserves exclusive rights to deny Service or consider Service delivery to fall under Not Managed Resource Support for any software, application, system, or other Technology Resource that does not offer MFA.

The Provider reserves the right to deny Service delivery for a specific request or requests, or fully discontinue all Service delivery for the Client should a security or cybersecurity incident occur and, at the sole determination of the Provider, the incident occurred due to the Client or a Client representative disengaging, disabling, bypassing, or otherwise removing the effectiveness of MFA or other security protocols recommended by the Provider.

The Provider considers any security breach, hack, disclosure of data or information, or any other security or cybersecurity incident occurring under or relating to an account, system, application, or software that was not protected under a Provider approved MFA to be the sole responsibility of the Client.

The Provider may advise the Client on technology security improvements and recommendations which may be presented as part of a technology improvement project falling under IT Project or IT Consulting. While the Provider makes every effort to classify projects and components of projects as related to technology security, a project may not have security listed as the primary title or header, but may still impact the overall security of the Client systems,

network, and cybersecurity risk exposure. The Provider has the sole discretion at any time to classify a project item as technology security related, including following a cybersecurity incident. The Client is responsible to approve and fund technology security improvement projects in a timely manner. Failure to implement recommended technology security improvements may result in greater risks for the Client. Cybersecurity incidents that could have been prevented by the implementation of a technology improvement project fall under Emergency Services and are not covered by Managed Services or Co-Managed Services.

16. **Insurance.**

Based on general business guidance and best practices, the Provider recommends most Clients carry a Cybersecurity Insurance policy. The Provider is not an expert, provider, reseller, or broker for insurance policies, including Cybersecurity Insurance. At the request of the Client, the Provider may make recommendations or offer counsel regarding insurance options, recommendations, or as part of a cybersecurity insurance application, audit, review, or claim, the Provider may provide the Client with technical information, procedures, or other technology-related information in support of the Client. The Client is solely responsible for understanding, vetting, approving, completing, and complying with any and all Client insurance documents, forms, applications, audits, etc.

The Client may request information from the Provider for insurance policy purposes, including, but not limited to, sharing an official insurance policy document, such as an audit form, insurance policy evaluation, or technology infrastructure or cybersecurity assessment. The Provider may provide recommendations or information based on information available to the Provider, and these recommendations or information may be provided to the Client directly within an official insurance policy document. It is the sole responsibility of the Client to review, understand, evaluate, modify, and approve any and all recommendations or information shared by the Provider. The Provider will never act as the signer, either directly or on behalf of the Client, on a Client insurance document.

17. **Indemnification.**

The Client shall defend, indemnify and hold the Provider harmless from any claim, suit, damages and expenses (including, but not limited to, attorneys' fees) arising out of the failure of the Client to comply with any and all software, hardware, or Third Party licenses, terms and conditions, agreements, and all applicable laws, rules and regulations.

To the fullest extent permitted by law, the Client agrees to indemnify, defend and hold the Provider and its owners, officers, employees, contractors, and agents harmless from and against any and all claims, suits, damages, losses, expenses, and actions of every name, kind and description, including, but not limited to, insurance claims, expenses, ransom demands, or recovery costs of any kind as a result of a cybersecurity events, such as a ransomware attack, costs associated with business interruption or with delays in software or hardware implementation, costs or actions resulting from the failure of network or data restoration, any sanctions, penalties, or claims of damages resulting from the Client's failure to comply, if applicable, with requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all Federal regulations promulgated thereunder, as amended, any sanctions, penalties, or claims of damages resulting from the Client's failure to comply, if applicable, with requirements set forth in the Payment Card Industry Data Security Standard (PCI DSS), court costs, attorney's fees, and alternative dispute resolution costs, for any personal injury, for any bodily injury, sickness, disease or death and for any damages to personal reputation, Client reputation, and for any damage to or destruction of any property, whether physical or electronic data, information, or systems (including the loss of use resulting therefrom) which 1) are caused in whole or in part by any action or omission, negligent or otherwise, of the Provider, its employees, owners, agents, or volunteers or Provider's subcontractors and their employees,

owners, or agents; or 2) are directly or indirectly arising out of, resulting from, or in connection with performance of this Agreement.