eGroupTech

# Response to CCOC Request for Proposal (RFP)
# For
# Outsourced IT & Managed Services/Support

FLORIDA CLERKS OF COURTS
CCOC
OPERATIONS CORPORATION

| | |
|---|---|
| Prepared for: | John Dew, Executive Director |
| Prepared by: | Kenneth Baker, C.M. – President<br>Kenneth R Baker |
| Date: | November 23, 2021 |

eGroupTech, Inc. | www.egrouptech.com

2441 Monticello Dr. Ste. 600 | Tallahassee, FL  32303

850-894-6400

***Table of Contents***

The remainder of this page is intentionally blank.

# ***Scope of Services: (2.0)***

**Executive Summary:** eGroupTech will continue to act in the capacity of a Managed Services Provider (MSP) for CCOC if this response for RFP is accepted and awarded to our organization. A managed service provider (MSP) is a company that remotely manages a customer's entire IT infrastructure, end-user systems, servers, software, help desk, e-mail, network security, incident resolution, new hardware build, configuration and installation, including vendor - purchase management, on a very proactive basis under a subscription model.

There are 45 comprehensive, connected methodologies for improving the core functions of IT within an organization. Each of these areas affects the business, stakeholders and the IT organization. eGroupTech has access to these resources as a result of our partnership with one of the major IT research firms. Some of this updated research was utilized and incorporated into the responses for the Scope of services requirements within this RFP. Technology Strategy Planning section 2.1.4 continues to incorporate some of the IT Governance Framework and IT Strategy. Additional resources as required from the research group can be utilized as part of the dedicated hours for CIO services to help CCOC in any IT areas of concern.

A Remote Management and Monitoring (RMM) application will continue to be utilized to support the services outlined in this RFQ. A remote network monitoring, management, and reporting solution that defines the actual network layer will be added to and integrated into the RMM application. The management and monitoring of Exchange on-line (e-mail) and Office 365 is also part of the solution. The RMM and supporting software contain agents and other software based probes that collect the data from the environment for reporting and alerts. eGroupTech will continue to furnish an administrative workstation for the CCOC network that will host and run the various components of the RMM software. This will continue to alleviate the burden of running support agents on CCOC production machines. Each CCOC machine is required to continue to run the core RMM agent.

Unlimited on site and remote technical assistance will be provided for troubleshooting and solving CCOC's technology issues [1 Appendix A]. Solutions may include the repair and / or replacement of physical devices, Microsoft Application Support, patch management software updates, driver updates, operating systems, anti-virus management, virus removal, router configuration, and the installation and configuration of new or upgraded software. Assistance will be provided for the integration of tablets, smart phones, and mobile applications into the CCOC environment as required.

This response to CCOC's RFQ contains several projects that will be updated with the current environment. They are: An updated IT environment Assessment; Additional consulting on IT Governance and Strategic planning with the result being a updated 3 year CCOC IT Strategic plan; Assessment of all CCOC data assets with recommendations that results in a 3 layer data safety / security process.; An update of the Cyber Security planning tool and outlining the best practices to protect CCOC that results in a updated security plan for the organization ; Completing a basic threat assessment as defined in the security section of the RFP to establish a current security baseline; and Continued development of a full set of IT Policy, Procedures and SOPs for CCOC.

## *Value Added Service Requirements: (2.1)*

In February of 2021 CCOC issued a Request for Quote (RFQ) Information Technology Department Review. Specifically of interest is scope of services 2.1 Review / Assessment of CCOC's "IT" department. CCOC has a current baseline of IT operations. One of the first items of business if this RFP is awarded to eGroupTech is to use the current baseline, and have a discussion about what: CCOC should plan for over the next three years. eGroupTech will then conduct a full assessment of CCOC's IT environment updating the document to the current state based upon the newest acquisitions over the past year.

eGroupTech is continuing to recommend additional assessments for several service requirements listed in this RFQ. Methodologies for updated assessments in the areas of Backup, Security Threat, and Policy development are listed in detail of the appropriate section of this RFP.

### *Remote Backup: (2.1.1)*

eGroupTech will continue to evaluate and consider how best to protect CCOC's data, prioritizing and establishing a multi-tiered backup and data recovery process consisting of current industry best practices. There continue to be multiple competing backup products and numerous vendors that all claim to be the best. Rather than picking out a backup product and then trying to configure it to protect an organization's data, it is better to develop a comprehensive backup strategy for CCOC and then figure out which product(s) will best fit that strategy. eGroupTech will re-evaluate the processes put in place and determine if there are better products and processes for the current environment

A successful implementation of this strategy requires a review of CCOC's current back up process(s) and all documentation. Based on that review, recommendations will be provided and a revised or updated plan established. The written back up plan will be updated that currently defines what is being backed up for each device or application; where it is being backed up; how often backups will occur; that backups are preformed according to the various schedules; and the processes are continuously monitored by the RMM software. Exceptions and alerts will be generated for any anomalies.

Getting *all* of the organization's data identified and located is an integral part of the plan. For example, while most Windows users store data in their Documents folder, they also may keep files and folders on the Desktop, which will need to be backed up as well. Special database or financial-software packages may store files in their program directories, so this type data needs to be identified and backed up, too. Some programs and hardware allow you to back up configurations or settings. Each application and device at CCOC will be reviewed to see if it supports this functionality and added to the plan.

Consideration must be provided for any work from home laptops or mobile devices that are in the field or off site. Just because they are out of the office does not mean the backups should be delayed or ignored.

E-mail is also part of the process. A full understanding of where any local and server e-mail is stored will be defined and included in the plan. Although OFFICE 365 e-mail in Exchange online provides individual item recovery and Microsoft redistributes the Exchange files in multiple data centers, the waring in their own documentation states: "*With all the previously mentioned options for Deleted item recovery, note that point in time restoration of mailbox items is out of the scope of the on-line Exchange service*". Although there have not been any e-mail box recovery issues over the past three years, CCOC needs to entertain an additional specific back up strategy for your Office 365 – Online Exchange Process.

CCOC employees have an extensive bookmark collection in their browsers; it will continue to be part of the overall backup plan. You may choose to periodically export your bookmark file from within the program, or point to the bookmark file itself in your backup software. A check of the individual browsers Help tools or consulting the web for details may be necessary.

In order for data and equipment to be adequately protected, there must be three copies of the data. The first copy isn't really a copy; it's the production data that is used every day on the servers, desktops or laptops. The second copy is a backup that you keep on site, and the third copy is an off-site backup that can be physical or cloud based. The data gets first written to really fast storage, where it's used during the time when it's accessed a lot, and [then] it migrates to slower storage, with a greater capacity and lower costs, and then it migrates down to tape or cloud. If you do that in a rigorous way, you end up with about 60%of your achievable data down at the tape / cloud layer, and that dramatically reduces the costs of your backup and recovery infrastructure.

The final plan will include a detailed process for file recovery and minimum testing of random file recovery on a quarterly basis.

## *Routine Software Updates: (2.1.2)*

Desktop, laptop and server software updates and patching will be provided by the RMM software. Options will be discussed and best practices will be presented in order to choose what routine software updates best suit the CCOC environment. Multiple system options are available to automate patching within desktop, laptop and server systems. Patches and software updates will be reviewed and predefine to determine which patches should be approved, if they should be staged, when they are to be installed, and how the patch agent should react in case of a required reboot of the hardware. If a particular software application should not be updated because a legacy application will not run on a newer version of that application, the RMM software can prevent that application from updating from the current version on a particular workstation needed to support present operations.

Gone are the days of Microsoft releasing updates, hotfixes, and rollups only on the second Tuesday of the month. Since the release of Windows 10, the update schedule is more fluid. eGroupTech's patch process can let your team know within hours of an applicable update being released.

Third-party software is one of the most common attack vectors for hacks and exploits. Our process has visibility into the industry standard CVSS at the National Institute of Science and Technology

(NIST), and goes beyond basic Microsoft patching with protection for commonly exploited third-party software.

It's essential to manage third party patching to close vulnerabilities and protect CCOC as part of its security process(s). The RMM application integrates third party patch management which allows the process to audit, patch, and document third party application updates. All third party patch definitions are deployed following best practices, with automatic daily downloads ensuring CCOC is always patched to the latest version. Third Party Patch Management is integrated with the RMM application providing patches for the following popular applications: Adobe Reader, Adobe Acrobat, Adobe Shockwave, Apple iTunes, Google Chrome, Oracle Java, PDF Creator, 7-Zip, Mozilla Firefox, Notepad++, VLC Media Player and several other applications. Unique CCOC applications that cannot be patched under the third party patch software will be patched on a manual basis at least quarterly or as a notice of vulnerability is identified.

## *Routine Security Assistance: (2.1.3)*

**Routine Security Assistance:**

Routine security assistance updates and audits rely upon a defined Security / Cybersecurity plan. Security assistance consists of managing and configuring the security oriented devices and software currently in use within the organization. The devices consist of modems, routers and managed/unmanaged switches. The software consists of the organizations current antivirus / anti malware application WebRoot and any e-mail software for spam filtering etc... Documenting the current configuration(s) of existing hardware and software is part of this RFP.

A better understanding of CCOC's requirements for security can be developed through the process of a threat assessment. Completing a basic threat assessment as defined below and a creation of a security plan is included as part of this RFP. The assessment will determine what digital assets CCOC has and list them all: including emails; client work files past and present; financial records; marketing collateral; staff information; project plans; schedules; customer data; contracts; and any other information you want to protect. A discussion about the security risks CCOC faces might result in a list of things like:

- Accidental damage, for example, dropping a tablet and breaking the screen
- Natural disasters such as flood and fire
- Employee negligence, for example, accidental file deletion
- Employee misconduct, for example, stealing customer data
- Crime, for example, a break-in at your premises
- External risks like malware attacks and industrial espionage
- Technical failure, for example, the death of a vital server
- Security policies

Once the security risks and digital assets are defined, eGroupTech will help you develop a security plan to mitigate the risks. CCOC might include things like the following:

- You are using Microsoft Office 365 but is it set up to: ensure that our mail gets swept for viruses; archived; and kept secure?
- Moving local desktop / laptop data to a central file server or mirroring local files to the server or nas.
- Discourage staff from storing information on their local PCs - even working copies
- Backup vital data every day. – Refer to 2.1.1 Remote Backup
- Storing critical customer and business information on a Software As a Service (SAAS) application.
- Only staff working on a given project will have access to that project's files.
- Restricting access to business information like the accounts and payroll to a limited number of people on a need-to-know basis.
- Setting up an encryption process on all company desktops and laptops to encrypt files in case they are lost or stolen.
- Assess your current AV solution and compare it to current market leaders and change it if needed.
- Establish automated software patching system / process[1]. - Refer to 2.1.2 Routine Software Update.
- Security-marking every laptop – Asset tags – Stolen laptop tracking software.
- Getting an alarm / locksmith company to audit your physical security, locks, and alarms once a year.
- Updating our internet use policy with your lawyers and train new staff about it.
- Ensuring everyone in the company is familiar with any CCOC IT security procedures.
- Hold yearly training for the whole company to keep security knowledge fresh – utilize phishing scam testing software + education.
- Spot-check regularly to make sure IT security is being taken seriously, and your protocols are being followed.

It's a reasonably simple exercise, but even a basic cyber security plan can save you a world of pain. eGroupTech has utilized a on line Cyber Security planning tool and has created a detailed planning guide for CCOC's use that covers the following areas: Privacy and Data Security; Scams and Fraud; Network Security; e-Mail; Mobile Devices; Employees; Facility Security; Operational Security; Incident Response and Reporting; Policy Development and Management; Cyber Security Glossary; and Cyber Security Links. This planning guide will be attached as an additional document when the RFP is submitted (it is not included because it is 44 pages long by itself).

[1] As many malware and unwanted programs are installed through vulnerabilities found in outdated and insecure programs, it is strongly suggested that your devices be scanned for vulnerable programs on your computer. One of the most important things a MSP in conjunction with the user can do to is keep their computer secure, by making sure they are using the latest security updates for Windows and all of the installed programs

**Non Routine Security:**

Defending networks from sophisticated cyber attackers today is not necessary optional. To protect a business appropriately, there is a long list of appliances and applications organization's should use , including, but not limited to: distributed denial of service (DDoS) protection, intrusion detection/prevention systems, web application firewalls, data encryption[2], data loss prevention, security information and event management (SIEM) systems, deep packet inspection and network analyzers.

The following Non Routine Security processes are not included as part of this RFP but are available as necessary or requested by CCOC as a Project. It is highly suggested that a SIEM project be requested and implemented within the first year.

Distributed Denial-of-Service (DDoS): A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

Intrusion Detection System (IDS): An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Web application firewall (WAF): A Web application firewall (WAF) is a firewall that monitors, filters or blocks data packets as they travel to and from a Web application. A WAF can be network-based, host-based or cloud-based and is often deployed through a proxy and placed in front of one or more Web applications. Running as a network appliance, server plug-in or cloud service, the WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic. This requirement should be includes in your web hosting RFP. Or for any web server that hosts or distributes an organizations data.

Security Information and Event Management (SIEM): Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. Security Information Management (SIM) is the practice of collecting, monitoring and analyzing security-related data from computer logs. A security information management system (SIMS) automates that practice. Security information management is sometimes called security event management (SEM) or security information and event management (SIEM). Security information includes log data generated from numerous sources, including antivirus software, intrusion-detection systems (IDS), intrusion-prevention systems (IPS), file systems, firewalls, routers, servers and switches. Security information management systems may: Monitor events in real time; Display a real-time view of activity; Translate event data from various sources into a common format, typically XML; Aggregate data; Correlate data from multiple sources; Cross-correlate to help administrators discern between real threats and false positives; Provide automated incidence response; Send alerts and generate reports.

Data loss prevention (DLP): is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission. Adoption of DLP is being driven by insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. In addition to being able to monitor and control endpoint activities, some DLP tools can also be used to filter data streams on the corporate network and protect data in motion. DLP products may also be referred to as data leak prevention, information loss prevention or extrusion prevention products.

Penetration testing and vulnerability assessments: This includes one-time or periodic software scans or friendly hacking attempts in order to find vulnerabilities in a technical and logical perimeter. It generally does not assess security throughout the network, nor does it accurately reflect personnel-related exposures due to disgruntled employees, social engineering, etc.

Any type of Unified Security Management tools (USM) or processes.

Managed Security Service Providers MSSP contracts and / or MSSP Software and appliances can be layered into your IT environment. Any form of a Unified Security Management tool (USM) provides information in a single security dashboard. One can easily perform network vulnerability assessment in your cloud, on-premises, and hybrid environments. It brings together essential security capabilities: asset discovery and inventory; vulnerability assessment; intrusion detection; behavioral monitoring; SIEM; and log management all in a unified, easy-to-use platform. In addition, continuous threat intelligence, including vulnerability signatures, can be delivered to the application directly from specific Security Research Team(s).

Although it was not a requirement of this RFP, eGroupTech researched including MSSP services into the RFP. A full MSSP / USM solution would add 7 to 9k per month to the costs if included.

[2] eGroupTech has suggested encryption in the routine security assistance section

## *Technology Strategy Planning: (2.1.4)*

Developing an appropriate technology strategy should not be completed without addressing IT Governance and its impact upon IT Strategy. IT Governance: Is the process of guiding the executives of an organization to align IT with overall business objectives and processes.

IT governance is the number-one predictor of value generated by IT, yet many organizations struggle to organize their governance effectively.

- Current IT governance does not address the changing goals, risks, or context of the organization so the dollars spent for IT are not easily linked to value.
- The right people are not / may not be making the right decisions about IT.
- Organizations may not have a governance framework in place that optimally aligns IT with the business objectives and direction.

- Implementing IT governance requires the involvement of key business stakeholders who do not always see IT's value in corporate governance and strategy.
- The current governance processes may be poorly designed, making the time to decisions too long and driving non-compliance.
- eGroupTech's governance methodology: supports the enablement of IT business-alignment; decreases decision-making cycle times; and increases IT's transparency and effectiveness in decisions around benefits realization, risks, and resources.

The following four-step process for optimizing your IT governance framework will be introduced at the CIO consulting meetings with CCOC's executives.

Successful completion of the IT governance redesign will result in the following outcomes:

1. Align IT with the business context.
2. Assess the current governance framework.
3. Redesign the governance framework.
4. Implement governance redesign.

IT Strategy: IT strategy (information technology strategy) is a comprehensive plan that outlines how technology should be used to meet IT and business goals. An IT strategy, also called a technology strategy or IT/technology strategic plan, is a written document that details the multiple factors that affect the organization's investment in and use of technology. It should cover all facets of technology management: including cost management; human capital management; hardware and software management; vendor management; and risk management.

A strong IT strategy provides a blueprint of how technology supports and shapes the organization's overall business strategy. Its strategic goals should mirror business projects (aka business alignment) and take into account the needs of key stakeholders including employees, customers and business partners.

The strategy should offer a look at the organization's current technology posture and provide an idea of where IT should head over the next three to five years.

There are different models that help executives of an organization construct an IT strategy, yet most contain certain key elements including:

- A high-level overview of the IT department that covers its mission, core values, objectives and approaches to accomplishing its goals.
- Current budgets and spending forecasts for a multiyear timeline.
- An outline of current and future IT projects and initiatives with timelines and milestones.
- A catalog of existing enterprise architecture; IT department capabilities and capacities; and future needs and requirements with details about infrastructure, staffing and other necessary resources.
- An analysis of IT's strengths and weaknesses utilizing a SWOT analysis (Strengths, Weaknesses, Opportunities and Threats.

- A list of the internal and external forces (such as market and industry trends) that shape current technology requirements and innovations as well as the future forces expected to shape IT.
- A prediction of the potential opportunities and vulnerabilities that will necessitate technology responses to best position the organization for success.

The importance of an IT strategy has been amplified over the past few years as organizations focus on digital transformation and thriving in the digital age. Technology is essential for creating new business models, new business processes, products and services; enhancing customer service as well as customer experiences; increasing sales; enabling workers and improving productivity; and supporting interactions with vendors and other business partners.

Just as there are varying models for the document itself, there are multiple ways to approach the creation of an IT strategy. Still, commonalities exist, such as an initial review of the organization's existing strategic IT plan and related documents.

This step should be followed by an assessment of how the organization is meeting established objectives, milestones, benchmarks and relevant key performance indicators. This assessment should identify the technology currently in use and the gaps that exist between these current IT operations and the objectives and strategic goals outlined in the ongoing strategic plans.

The process requires the need to collaborate with the organizations business-side counterparts to further develop the IT strategy. They should also seek out other resources, such as research reports, to understand the business and technology trends that will impact their organization's market.

All this creates the groundwork for the development of short-term and long-term objectives, budget projections, technology predictions and the perceived future opportunities and vulnerabilities that go into the technology strategy along with the corresponding summaries needed for the final document.

A strong IT strategy relies not just on creating the plan, but also on proper implementation of it. After all, these documents don't do any good if they're ignored after completion.

Adherence to the IT strategy should not be overly rigid. The fast pace of technology advancements and innovation require organizations to be agile if they want to seize upon new, and sometimes unforeseen, developments that can help them be more competitive or better serve their market.

Thus, the technology strategy needs to be flexible. IT and other line of business executives must also be nimble, and they should expect to reassess and redevelop the technology strategy at least annually and possibly revisit it even more frequently to, first, verify the tactical plans align with the technology strategy and, second, verify the technology strategy remains aligned with the overall organizational mission as it changes in response to shifting dynamics

Using the guidelines, methodologies and processes listed in this sections response, eGroupTech will consult with the Executive Director, Deputy Executive Director and all stake holders within the

CCOC organization. This process will be started within the first month and may take 4 to 6 months to compete a final document.

As a result of the Strategic plan, an operation budget needs to be created. eGroupTech has the capability of providing a 3 to 4 year IT budgeting process for CCOC once the strategic plan and parameters for the IT equipment Life cycle have been defined.

## ***Solution Design: (2.1.5)***

eGroupTech has an extensive background in business process engineering – reengineering. The proper integration of people, process and technology results in an efficient and effective organization. If CCOC has identified one or more technology requirements as part of the strategic planning exercises, or an opportunity in a SWOT analysis, eGroupTech will:

- Help define the enhancements to an existing business process;
- Define requirements and the technology (software, hardware , licensing and data) to support CCOC's development of a new process or product;
- Recommend newer solutions that may be Cloud based software as a service solution for one or more process that CCOC is currently using.

Software Licensing Management is covered in section 2.1.17 below.

## ***Network & E-mail Monitoring: (2.1.6)***

24/7 monitoring of the CCOC network and e-mail services will be accomplished within the RMM application or with specific software as a Service (SAS) application(s) integrated with (or additive to) the RMM tool. Alerts that are automatically generated will be sent to the RMM ticketing system, the eGroupTech Help Desk (or both) providing automatic notification to eGroupTech's technical support group before CCOC may be aware there is an issue. If any outage is noted, we will communicate it via e-mail or a specific call tree list. The standard help desk SLA process provides the escalation protocols based on the severity of any unscheduled outages.

### ***Network Monitoring: (2.1.6.1)***

eGroupTech's MSP services for this RFP include a remote network monitoring and management solution that is focused on our client's network infrastructure. The application is integrated into the RMM software and provides live visual information with device drill down. It provides constant monitoring of switches, routers, firewalls, and Wi-Fi controllers within the network infrastructure. It delivers unprecedented insight into client networks and automating time-consuming documentation and monitoring tasks. It is cloud based SAS software and is the ideal complement to existing RMM / endpoint management applications. It supports more than 7,000 devices from 230+ vendors. This SAS application has the capabilities to see and manage networks for multiple client locations. The client side of the SAS application installs on a local workstation within the CCOC network. Once installed the discovery process starts automated mapping, inventory, and configuration backup, generates alerting and statistics. Within 15 minutes of installation an infrastructure assessment is complete and eGroupTech will start making recommendations for improvements to the CCOC network.

Specific benefits are:

- Automated Topology & Documentation: Real-time automated network mapping and inventory will tell us exactly what's on the CCOC network (including serial number, firmware, etc.) and how it's connected.
- Monitoring & Alerts: 40+ preconfigured alerts are immediately available, allowing one to be in-the-know about network events that need attention. Need something different or a unique alert? We can shape the system to CCOC's network with easy customization.
- Configuration Management: The application automatically documents all the running infrastructure configurations and tracks them over time. It backs up router configurations and whenever there's a change it keeps all previous configurations allowing one to compare configurations with highlighted differences. One-click restoration instantly brings back any configuration from the version history.
- Troubleshooting Tools: ARP tables, FDB tables, and listed routes are all automatically generated by the application and pooled into one easy-to-access location. Superb design and smart filters allow you to zero in on what you're looking for among the raw data.
- Remote Access: With one click, instantly access nearly any Telnet-, SSH- or web-enabled device through a terminal, or remote browser, on the managed network utilizing the remote network monitoring and management dashboard.
- Bandwidth and Internet usage monitoring: Provides live and historical statistics for an individual device, network or network sub net indication if one or more devices are slowing down the network.
- Unprecedented Visibility: The remote network monitoring and management allows eGroupTech to be proactive not reactive!

## ***E-mail Management & Monitoring: (2.1.6.2)***

eGroupTech is an authorized Microsoft Partner and reseller of Office 365 services. We have the knowledge to analyze an organization and recommend the appropriate level of Office 365 and / or Office 365 Hosted Exchange Services. Several of our existing clients are on Office 365 Hosted Exchange. They were migrated from various on site or hosed e-mail services. Several have Office 365 and were migrated from older versions of Office.

Email has become a reliable and ubiquitous communication medium for information workers in organizations of all sizes. Messaging stores and mailboxes have become repositories of valuable company data. It's important for organizations to formulate messaging policies that dictate the fair use of their messaging systems, provide user guidelines for how to act on the policies, and where required, provide details about the types of communication that may not be allowed.

Organizations must also create policies to manage email lifecycle, retain messages for the length of time based on business, legal, and regulatory requirements, preserve email records for litigation and investigation purposes, and are prepared to search and provide the required email records to fulfill eDiscovery requests.

Leakage of sensitive information such as intellectual property, trade secrets, business plans, and personally identifiable information (PII) collected or handled by your organization must also be protected.

CCOC's Hosted Exchange (Office 365) could / can be manually configured to send statuses of the health of the system and other alerts. The default installation of Hosted Exchange includes a very minimal set of implementations for monitoring and management.

eGroupTech will continue to include a Hosted Exchange and Office 356 monitoring and management tool in this RFP. OM Plus is a comprehensive hosted Exchange e-mail - Office 365 tool used for reporting, managing, monitoring, auditing, and creating alerts for critical activities. It manages Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Office 365 services all from one place.

OM Plus provides exhaustive preconfigured reports on hosted Exchange e-mail - Office 365 and helps perform complex tasks including bulk user management, bulk mailbox management, secure delegation, and more.

OM Plus monitors Hosted Exchange - Office 365 services around the clock, and generates instant alerts / email notifications about service outages. OM Plus eases compliance management with built-in compliance reports and offers advanced auditing and alerting features to keep your hosted Exchange e-mail - Office 365 setup secure.

OM Plus reporting provides over 200 preconfigured reports on hosted Exchange e-mail - Office 365. It consolidates data from Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, and other Office 365 components into detailed reports, giving you complete visibility into your Office 365 setup. The reports can be scheduled and exported to PDF, CSV, XLS, or HTML format.

With OM Plus reports, monitor mailbox traffic and understand Exchange Online adoption inside your organization. Identify malicious spam emails to keep your Exchange Online environment secure. Identify inactive users, soon-to-expire licenses, and soon-to-expire passwords with reports on Azure Active Directory to take preemptive actions and avoid unexpected consequences. View Skype for Business and OneDrive for Business usage statistics. Ensure that IT compliance standards like SOX, PCI-DSS, HIPAA, GLBA, and FISMA are met with the help of compliance reports.

OM Plus auditing monitors every event happening in your Hosted Exchange - Office 365 environment to take preemptive actions and avoid dire consequences. Know who did what operation and when. Get a clear report of user activities on all hosted Exchange - Office 365 components in one place. With OM Plus auditing, keep track of user log on and log offs to monitor Office 365 users' behaviors. Monitor critical license changes made by users, to avoid license-related issues. Monitor even the smallest attribute changes made by users including mailbox permission and property changes in order to keep the Exchange Online environment in check.

With OM Plus alerting, get notified about critical activities and changes happening in your hosted Exchange e-mail - Office 365 environment. OM Plus lets one to create custom alerts for each Office

365 service. These custom alerts save time by eliminating the need to constantly check audit reports for malicious activities.

OM Plus lets you: Create custom alerts for specific actions. Specify whether all mailboxes or only select mailboxes need to be monitored for suspicious activity. Create your own custom alert messages to send to administrators. Email administrators about which action triggered an alert to help them locate the source of the action immediately.

## *Procurement Management: (2.1.7)*

eGroupTech's procurement process helps its clients manage the entire product procurement lifecycle in a way that reduces mistakes and creates accountability when tracking items.

Our procedure consists of 5 main processes: selection of equipment based upon client requirements or standards; purchasing from designated supplier(s), or third part market place; placing the purchase order; Receiving and documenting items; and inventory/ asset reports.

- set up a CCOC client quote system
- Setting up purchasing, receiving, and inventory defaults for CCOC
- Creating purchase orders
- Receiving products identification / validation to Order, Packing slip and invoice
- Importing any products and asset information into the RMM system (if not auto discoverable)

eGroupTech will coordinate any equipment returns whether they are warranty or repair. Ordering replacement parts utilizes the purchasing process as defined above.

CCOC can purchase their items directly if they wish and have them drop shipped to eGroupTech. We will take care of the Receiving and documenting of the items; and provide the inventory/ asset reports.

## *Move – Add - Change: (2.1.8)*

Moves, Additions and Changes (MAC) are part of the managed services contract. Once a MAC help desk ticket is opened with a designated request for reasonable completion date, a check list of appropriate tasks will be generated. The task list is different depending upon what type of MAC is requested. The following types of MAC activities are part of this RFP.

- New user adds removes and changes to workstations including access to devices as necessary
- New user adds removes and changes to servers / AD including access to resources as necessary
- New user adds removes and changes to network based devices (printers or scanners) including access to devices as necessary
- New user adds removes and changes including access to the RMM application, network monitoring , OM Plus and/ or any other RMM application requiring end user identification

- New user adds removes and changes to Office 365 and Hosed exchange including e-mail box creation, archiving or deletion
- New user adds removes and changes to work from home laptops
- Relocating a computer from one office to another (without user changes)
- Relocating a computer from one office to another (with user changes)

## Warranty, Break Fix & Installation: (2.1.9)

### Warranty: 2.1.9.1

Technical support for any devices that are within a covered OEM warranty are part of the managed services contract. Once a help desk ticket is opened describing the issue and a designated service level selected, an assigned technician will: establish a call with the appropriate vendor; get a vendor ticket number; coordinate with the appropriate vendors customer support personnel; run any tests or diagnostics requested by the OEM support personnel. If replacement parts are needed the technician will document the order number and expected delivery date and update the ticket indicating the current status of the issue. If on-site support is needed the technician will coordinate the OEM representatives time and date of onsite arrival and be at the CCOC offices to verify that the appropriate work is being completed so the unit can be placed back in service.

### Break Fix: 2.1.9.2

Break / Fix operations are part of the managed services contract. The following types of Break / Fix activities are part of this RFP.

- Provide emergency remote and on site break / fix operations for desktops, laptops and tablets in the office or work from home locations
- Provide emergency remote and on site break / fix operations for workstation peripherals
- Provide emergency remote and on site break / fix operations for servers
- Provide emergency remote and on site break / fix operations for router and switches

Emergency response to server issues will be according to the SLA and the type of designated service level required for the incident. A server wont boot will be a level 1 incident. The server has an amber light on one of the drives will be a level 3 or 4 incident.

### Installation: 2.1.9.3

Installations are part of the managed services contract. The following types of installation activities are part of this RFP.

- Install and troubleshoot workstations including workstation OS, device drivers and connectivity
- Install and troubleshoot workstation applications. Support and troubleshoot all standard software including Adobe products, MS Office, and other software as determined by the list of specifically included software - workstation in Appendix A-S1

- Installation, monitoring and verification of workstation data back-up including logs / alert monitoring as requested

- Install and troubleshoot servers including OS, device drivers and connectivity

- Install and troubleshoot server applications. Support and troubleshoot all standard software or software with server components, and other software as determined by the list of specifically included software - servers in Appendix A-S2

- Installation, monitoring and verification of server data back-up including logs / alert monitoring as requested

- Install and troubleshoot Router and switches and connectivity

## ***Help Desk – Office and Remote: (2.1.10)***

eGroupTech has implemented a Zendesk helpdesk ticketing system for use. It makes it very straight forward for end users to submit a help desk ticket. Individual CCOC users and / or a designated individual will be required to submit all Managed Services / IT requests to helpdesk@egrouptech.com. If Internet access or e-mail is not available from any workstation or mobile device, please phone in your help desk request to 850-894-6400. Your request will be entered onto the help desk system, and a ticket generated for you and sent to the e-mail address on file for the requestor.

For help desk "Priorities" and the covered / categorized work descriptions please see below:

**eGroupTech - Help Desk Ticket Work Order Priorities**

When users experience problems, the eGroupTech’s Managed Services help desk group makes every effort to resolve the matter in a timely fashion. In order to triage the end user requests and make sure individuals requiring immediate attention are serviced in a timely manner, the following list of the priorities are utilized by the Help Desk to categorize each problem:

1. Level1 - (ASAP - immediate response) Critical Impact/System Down: Business critical software component is inoperable or critical interface has failed. This usually applies to a production environment and indicates you are unable to use the program resulting in a critical impact on operations. Downtime cannot be tolerated and the device / service must be online as quickly as possible. This includes connections to the Internet, email server is down / major issues, virus outbreaks, or other problems that affect / prohibit all users in the business from performing assigned tasks. Note: We will work with you 7x24 to resolve critical problems providing you have a technical resource available to work during those hours.
2. Level2 - (High immediate to 1 day response) this category covers many of the same issues as ASAP group. If the issues are affecting a single or limited numbers of users or the person responsible for the assigned ticket has higher level issues to resolve before troubleshooting this issue. Level 2 items are classified as having a significant business impact: A software

component is severely restricted in its use or you are in jeopardy of missing business deadlines because of problems with a new application rollout.

3. Level 3 - (moderate 1 to 3 day response) some business impact; Indicates the program is usable with less significant features (not critical to operations) unavailable. This category covers equipment moves, new user account setup, printer issues and other peripheral installation and troubleshooting, a client cannot connect to a server, inter-departmental connectivity, and wired and wireless connections.

4. Level4 - (Low 4 day to 1 week response) Minimal business impact: A non-critical software component is malfunctioning, causing minimal impact, or a non-technical request is made, researching software, documentation is incorrect, additional documentation requested, clean-up of user computers and general system/network housekeeping.

All help desk tickets will be resolved via remote access whenever possible. If a Level one issue arises and on-site service is required the same SLA time frames apply. If the issue is known and eGroupTech has known good spares or new in stock items, we will bring them with us to the on-site visit so the issue can be resolved in one on-site visit.

A service-level agreement (SLA): is an arrangement between the managed service provider and client indicating that the service provider will deliver a certain level of support based on specific parameters, such as the severity and frequency of a problem, as well as the time of day when the problem occurs. An SLA is essentially a health or life insurance policy for the clients IT computers, server and network.

**eGroupTech - Technical Services Service Level Agreement (SLA)**

| SLA Level | SLA Response Time |
|---|---|
| Level 1 | 24/7/365, 1.5 - hour response - except Designated Holidays 4hour response remote only |
| Level 2 | 24/7, M-F 4hour response |
| Level 3 | 8x5, next-business day response |
| Level 4 | 8x5, next-business week response |

**eGroupTech - Business and Support hour's definition**

| | |
|---|---|
| **Normal business hours** | are defined as Monday to Friday beginning at 8:00 AM and ending at 5:00 PM EST. |
| **Weekend support** | is defined as 5:01PM Friday through 7:59 AM Monday |
| **After hours support** | is defined as 5:01 PM to 7:59 AM Monday through Thursday |
| **Holiday support** | is defined as any national published holiday. If the celebrated holiday falls on Monday or Friday, the Holiday rate will apply. |

## *Reporting & Communication: (2.1.11)*

As with any relationship, communication between an organization and a service provider is crucial to ensuring both parties are getting what they need.

For things to go well with an MSP, it's all about the relationship. Organizations that do their part to keep the relationship strong through clear communication, reasonable terms, reasonable requests and documented expectations are more likely to have a positive experience.

Having regular relationship meetings with the provider that focus on the review of transferred risks, controls developed to mitigate risks and key metrics to determine acceptable management of transferred risks keeps everyone on the same page.

When things go wrong it's important to talk frankly about the issues, expectations and what both parties can do to work together to make it better. Go back to the contract and make sure that both parties understand what is written. Too often, a wall will be built between both sides and the relationship will quickly deteriorate. When this happens, things usually get worse – not better.

eGroupTech will schedule quarterly state of the system meetings with appropriate CCOC personnel. These meetings will be in addition to the CIO services and planning meetings that have been outlined in the RFP. Monthly or on demand meetings may be requested at any time by opening a help desk ticket containing the subject matter to be discussed.

The RMM system, integrated applications and management platforms can generate almost any type of report that may be required. eGroupTech suggests narrowing the actual reports down to a group that will provide meaning full data and metrics to CCOC on an ongoing basis. Specific Incident / issue reports can be generated for status on issues. Other reports like hardware and software reports will be run quarterly and added to the physical documentation binder. Help Desk reports containing the ticket information, resolution and time to complete are available. A summary of SLA data will be extracted monthly and provided with the next month's invoice for services.

Any new purchases will be documented with the PO, packing slip and invoice if purchased for CCOC by eGroupTech. If purchase was made directly by CCOC the organization must furnish this information so the asset lists for hardware or software can be updated. If this information needs to be feed to the RMM application or one if it's components, eGroupTech will update the documentation.

If CCOC has requested and signed an authorized Change Authorization Order (CAO) for additive new hardware, software, or other IT processes, a Project report on the status of that CAO will be provided monthly until the project is complete.

## *IT Policy Review & Development: (2.1.12)*

Policies, procedures, and standards each have their specific purposes and functions within the context of corporate IT governance. eGroupTech will help you find the right **balance** between

**policy and process.** Our intention is to understand your risk landscape and to identify key policy areas. In areas where policy is not necessary, we will establish SOPs, best practices, and guidelines to prescribe the IT behavior CCOC is looking for from its employees.

- Our approach starts by re-assessment of the current policies, procedures and SOP's
- This assessment will identify policies that are out of date, disorganized, and complicated. This assessment will utilize the Swim lane diagram Exhibit A on page 22
- If CCOC's current policies do not reflect current regulations and don't actually mitigate your organization's current IT risks they will be dis-guarded or rewritten.
- It's a misconception that your most severe risks each need a specific policy – SOPs, standards, and guidelines can be written to fit under your policy umbrella.
- Review of current policies will be followed up with a discussion for new policies to address ricks that are / may be identified. By aligning your policies with your greatest risks you will actually mitigate your organization's current IT risks.
- eGroupTech will write your policies on the right level – policies need to be understandable to the parts of the organization they affect.
- An IT policy review process will be established – to reassess the effectiveness of your IT policies on a regular basis so you know they still enable your critical procedures.

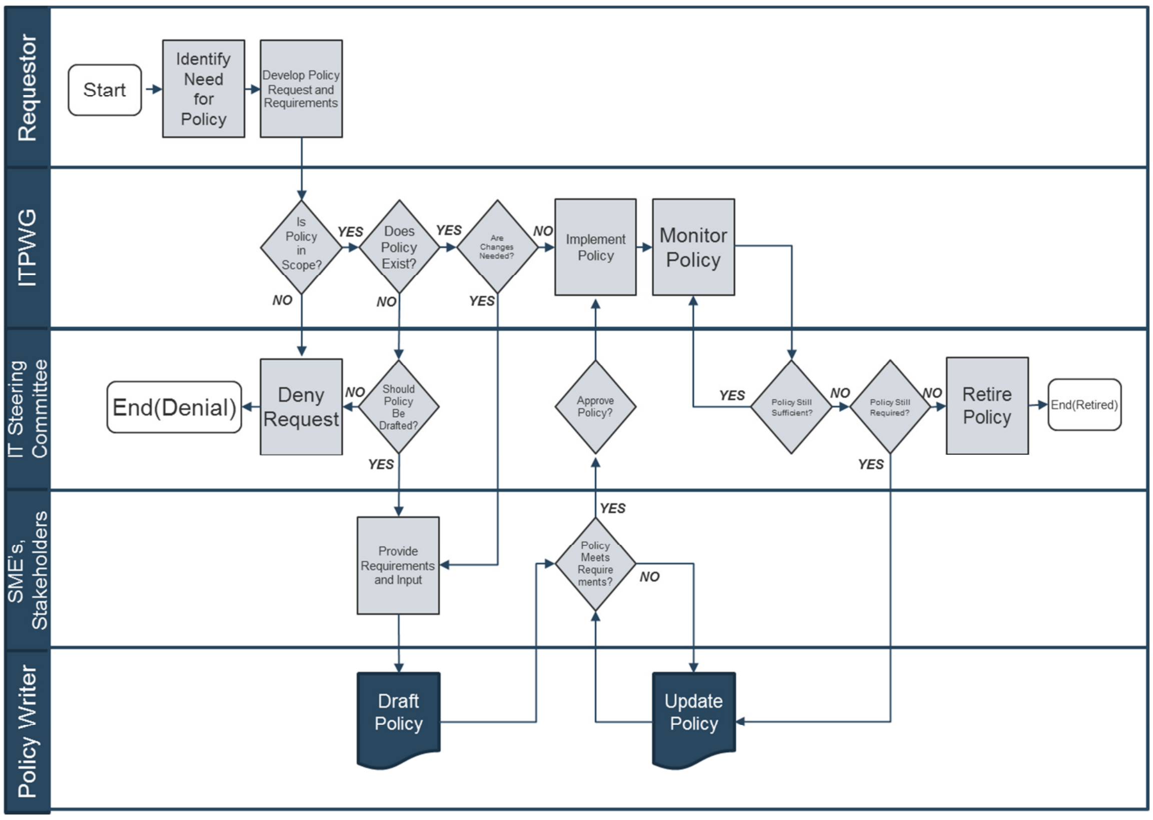
This process will develop an avenue for policy communication and make your policies available for reference in one place at any time. We will listen to the feedback you get from CCOC employees and talk it out. The best way to get buy-in is to make your employees part of the policy process - use their feedback and analysis to revise your policies. If your policies are difficult to understand, aren't easy to find, or aren't well monitored and enforced for compliance. They result in an atmosphere where your employees don't care about your policies.

eGroupTech's dynamic and streamlined policy approach will:

- Right-size policies to address the most critical IT risks.
- Clearly lay out a step-by-step process to complete daily tasks in compliance.
- Obtain policy adherence without having to be "the police."
- Address areas like: Acceptable Use Policy (AUP), Security Awareness, Information Security, DR/BCP, Change Management, Incident Response, BYOD, Vendor Access, Media destruction, retention & Backups

The remainder of this page is intentionally blank.

Exhibit A: Standard IT Policy Swim Lane assessment Diagram



## Unit Evaluation and Testing: (2.1.13)

If new hardware is presented to eGroupTech for test and evaluation, it will be taken to eGroupTech's the lab and the appropriate system or components will be compared against requirements and specifications through testing. The results are evaluated to assess progress of design, performance, supportability, etc. A report of the results will be provided to CCOC.

## Configuration: (2.1.14)

Any new hardware or software purchased on behalf of CCOC or directly by CCOC will be either drop shipped to the eGroupTech office or picked up from CCOC by an eGroupTech representative and transported to the eGroupTech Lab. Technicians at eGroupTech's lab will utilize a build sheet for each type of device for CCOC's network. A router or managed switch may use a generic build template. Servers will have a custom built template created for each individual server and go through a similar procedure as the workstation process described below.

Workstations will utilize a specific build template based upon CCOC's recommended standard hardware and software components and the role or department where the device will be used. Actual configuration of the hardware will utilize the check sheet step by step until the OS is configured, an Administrative user is created and the equipment is joined to a network. The next steps on the check sheet involve installing all standard software with any configuration that is required. The next steps involve the installation of unique software based upon department or end users requirements. The hardware is left on the bench to get any additional or new Microsoft updates. Updates for additional Office products are turned on and updates for Office 365 start. The core RMM software agent is loaded and the RMM console is checked to see that the device appears properly, has reported in and can be seen via remote access. Any software, printer drivers or special applications that will be needed on site but cannot be loaded until the hardware is on site within the CCOC offices, and physically joined to the CCOC domain is copied to an IT Downloads folder at the root of c:\ drive. All devices will be repackaged in the original boxes or shipping containers and scheduled for delivery to CCOC for onsite installation.

## ***PC Development: (2.1.15)***

Prerequisite to this process is RFP section - Configuration 2.1.14.

eGroupTech's process for hardware delivery and on site set up consists of:

- Unpacking the desktop. laptop or server
- Hooking up the Ethernet cable and / or joining the machine the local wireless network and identifying the CCOC network as the WORK network within the NIC.
- Joining the hardware to the CCOC domain with the appropriate credentials for the primary assigned user
- logging in as the assigned user and:

    - Set up Outlook e-mail account for primary assigned user
    - Map network drives according to primary assigned user assigned security group
    - Install all standard network based printers and test print a page
    - Install and test all local hardware - local printers, scanners, wireless mouse and keyboard if required – Set up external drives if necessary
    - Install, configure and register any unique / non-standard software for the assigned users job function

- Arrange desktop and put shortcuts for the most used programs on the desktop and in the task bar.
- Delete the standard junk from the users menu and frequently used programs list – turn off the newly installed programs feature in the menu
- Export or otherwise copy the favorites and bookmarks from the old desktop or laptop to the new desktop or laptop
- Physically install the laptop, docking station and related equipment on the assigned users' desk
- Provide the assigned end user any documentation, manuals or CD's – And/or add them to the documentation area within the CCOC office.
- Sit with the assigned user and go over anything new with this hardware compared to the end users previous device.
- Dispose of and boxes, plastic, packing materials and any extra cables or other materials

## Life Cycle Management: (2.1.16)

The scope and complexity of IT lifecycle services have changed significantly in recent years. Today, IT leadership deals with more devices, more applications, and a wider variety of workflows than ever before.

Two questions arise at the end of your IT equipment's lifecycle. First, how do you protect sensitive data on the hard drive? Then, how do you dispose of the asset? Our extensive program offerings provide options for every aspect of managing CCOC assets—from recycling and trade-in to environmentally friendly disposal. Once a piece of equipment is identified we will take care of the rest.

eGroupTech's Managed Services is ready to help you tackle the toughest, complex asset management tasks from asset disposition to warranty and installation. CCOC can rely on dependable; secure IT Asset Disposition through one of eGroupTech's partner ships with multiple recyclers. CCOC has the choice of a DOD level 5 wipe or shredding of the hard drives removed from your equipment. Once the hard drives are removed or rendered clean, the workstations can be donated to a local charity, sold in the open market or broken down into components for green recycling.

Once the standardized hardware and software lists are established for CCOC, the specific vendor life cycle information for software – hardware is gathered from their OEM web sites and put in a Bookmark folder on the Administrative workstation for reference. These links are utilized in the strategic and operational plans for guiding IT replacement decisions for workstations and software.

## Software Licensing Management: (2.1.17)

Software asset management (SAM) is the administration of processes, policies and procedures that support the procurement, deployment, use, maintenance and disposal of software applications within an organization. SAM is the part of IT asset management that seeks to ensure the organization complies with license agreements and does not overspend on software.

An important goal of every SAM initiative is to facilitate the discovery of software assets, ensure the validity of end user license agreements (EULAs) and validate the appropriate use of free software. SAM documentation can protect the organization from anti-piracy litigation, prevent the unintentional overuse of licenses and provide a control for shadow software on the network.

eGroupTech will be responsible for renewing software licenses, negotiating new license agreements and identifying and eliminating software that is rarely or never used.

The RMM application will auto discover all software on a workstation or server and reports can be generated to determine quantities and version levels of applications that are in use. If a database or spreadsheet of software purchased does not exist, CCOC is responsible for assembling all historical software purchase information and create this document. Once the as installed and as purchased information is available the issue of licensing compliance can be addressed.

All of CCOC existing software licenses that require annual or other renewal periods will be identified and entered into a IT calendar with 30 day setbacks in order to have the renewal licensing in place prior to the expiration of the existing term.

## ***Warehousing: (2.1.18)***

Where eGroupTech has sold three or more of exactly the same type of equipment to one or more of our clients, we maintain at our cost a set of known good spares in our inventory. As an example we have clients that utilize HP DL380 servers. We maintain a minimum of 3 each 146 GB, 300 GB and 600 GB spare hot pluggable drives.

We maintain sets of new: monitors in multiple sizes (23", 27" 32"); APC power supplies of various power levels (450, 750, 1500); 1GB capacity switches with 5,8,16 and 24 port configurations; Laptop & Desktop SSD drives in 128, 240 and 500mb capacity; replacement batteries for and APC / UPS power supply's we have sold; new Video cables of any configuration, Ethernet patch cables and other items.

eGroupTech's support truck carries a defined set of most used service call items. The truck has a standardized inventory stock list that is replenished if items are used in a service call. Some of the items on the truck are 5 and 8 port switches, video cables, power cables, Keyboards, wired and wireless mice, graphics cards, CMOS batteries and patch cables in various lengths.

eGroupTech can maintain either at its office or onsite a specific list of standardized spares that will be identified during the planning for CCOC IT.

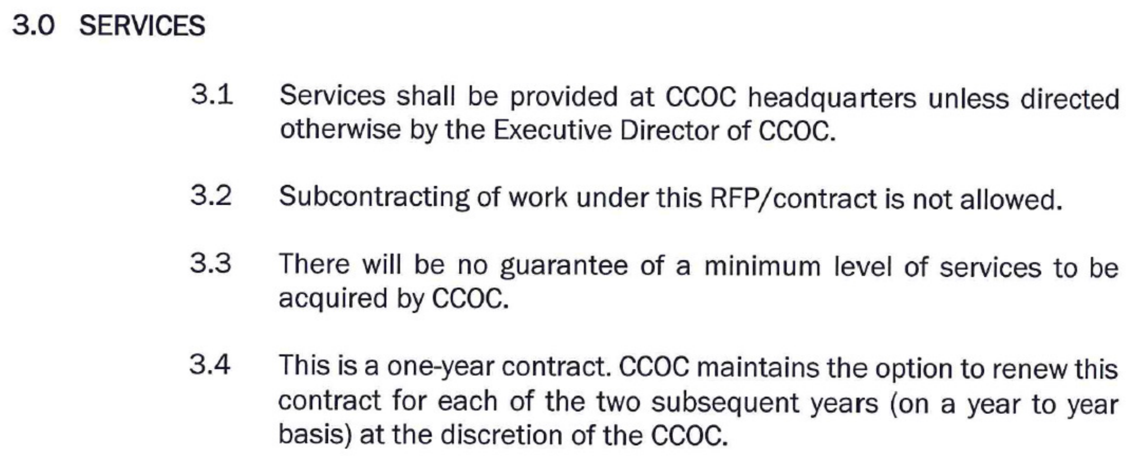
We also have a variety of off lease / used equipment. Currently there are servers, desktops, laptops, and some switches. We always have one or more laptops ready to go that can be put in service in an hour or less.

eGroupTech has designated devices available exclusively to its MSP clients that can be put into temporary service if there is a catastrophic failure of a laptop and the client does not have any of its own designated spares. Configuration and installation of the device to the client's network is covered as part of the MSP services.

Monthly IT Managed Services Fees do not include the cost of new or replacement hardware, software, software as a service, cabling or other equipment that may be required to perform services under this agreement. CCOC may procure equipment independently or a quote can be furnished for new or replacement equipment. CCOC will pre-approve all software, software as a service and equipment purchases. Purchases on behalf of CCOC by eGroupTech will be billed separately from the MSP contract at the end of the month or when the order is placed if the purchase price exceeds $500

Carrying a list of most used items on our support truck allows us to finish an onsite support call in one visit. This solves CCOC issues sooner, puts your environment back in service quicker, and is more efficient on our part.

## Services: (3.1 to 3.4)



3.0 SERVICES

3.1 Services shall be provided at CCOC headquarters unless directed otherwise by the Executive Director of CCOC.

3.2 Subcontracting of work under this RFP/contract is not allowed.

3.3 There will be no guarantee of a minimum level of services to be acquired by CCOC.

3.4 This is a one-year contract. CCOC maintains the option to renew this contract for each of the two subsequent years (on a year to year basis) at the discretion of the CCOC.

## Qualifications: (4.0)

eGroupTech's demonstrated experience and proficiency for managing and supporting information technology services is outlined in Sections 4.1 to 4.7

## PC Installations: (4.1)

eGroupTech has deployed and configured PC based equipment for companies starting in 1980 with the original IBM PC with dual floppy drives and running MS DOS. There is little resemblance to today's equipment other than the PC moniker. We regularly specify order, configure and deploy PC's and Apple based desktops, laptops, ultra-lights, 2 in 1's, all in One's, tablets and smart devices for our clients. We support the installation of these devices in LAN, WAN, VPN, Wireless, 4G and 5G networks.

## Troubleshooting / Hardware issues: (4.2)

eGroupTech provides on-site, remote and in lab troubleshooting of software and hardware issues for its current client base. Years of hands on experience leads a tech to not spend an inordinate amount of time trying to fix it. We understand and use the various vendors built in hardware diagnostic tools. Business-class systems from Dell, HP and IBM include their own diagnostic tools with their computers, either in the BIOS or on a disc. Understanding where to find and read various log files generated by diagnostic tools is critical. eGroupTech recommends standard hardware for clients because it makes the hardware troubleshooting process easier. Having known good spares available allows one to eliminate suspected components if they work correctly in a like machine. If eGroupTech sells more than three of the same type of workstation, laptop or server into its client base, we stock known good working spare parts that are available for replacement or testing.

One has to go through potential problems component by component, matching symptoms to issues and eliminate suspected problems in order to find the root cause of the issue and solve it.

Recognizing whether an issue is a hardware or software related is sometimes challenging as the errors are similar and can be caused by either. Having a suite of additional tools that you trust and use regularly during diagnosis provides client value by reducing the total cost of fixing the issue for the client.

## Software installation, re-imaging, configuration needs: (4.3)

eGroupTech has collected an extensive library of software including an archive of older software that may be required by a client for installation, re-imaging, or re-configuration. We have reconstructed a windows 2000 SP4 workstation and redeployed it as a replacement for a unique PC that was the controller for a 500k printing press. The success of this project saved the client from the purchase of a new software system for the press that would have cost 25K.

Each eGroupTech client has a standardized list of applications software for each type of device. We organize copies of each client's software into their unique software library. Unique applications are also downloaded and stored in the client software library. We maintain older version of the applications in case a workstation needs to be rolled back to an earlier version due to a software incompatibility.

eGroupTech has invested in data recovery software and hardware and has developed it's "drive rescue services". We have the equipment to clone and image drives, and to recover data from drive failures caused by software and boot issues. If White Room drive recovery is necessary because of a physical hardware failure, we have multiple relationships with drive recovery vendors to help recover your data. With eGroupTech's managed services a white room recovery services will probably never be needed once appropriate back up processes and procedures have been implemented.

## Supporting multiple hardware manufacturers: (4.4)

eGroupTech's client base utilizes recommended, installed and supported servers from HP, Dell, and IBM (Lenovo) and custom built servers.

Installed and supported client workstations and laptops are from Dell, HP, Toshiba, ASUS, Lenovo, Apple and custom built PC's. Tablets are I-pads, HP, Lenovo, Dell, and Samsung. For each device deployed to an eGroupTech client, a series of support documents including specifications, user and repair manuals are added to the client's documentation. eGroupTech is an authorized Dell and Lenovo Reseller and have partnerships with multiple channel suppliers.

eGroupTech's client base utilizes recommended, installed and supported routers from Cisco, D-Link, Avaya, 3COM, Linksys, Meraki, Netgear, TP-Link, Ubiquity, and ZyXEL. Switches from Cisco, Dell, d-link, EnGenius, Fortinet, HP Linksys, Meraki, Netgear, OpenMesh, TP-Link, Ubiquity, and ZyXEL

eGroupTech's client base utilizes recommended, installed and supported Network Area Storage (NAS) devices from Segate, QNap, Western Digital and Buffalo.

## *Supporting Server OS: (4.5)*

eGroupTech's client base includes installed and supported server operating systems starting with windows server 2012R2. Our managed client base requires support for the following Windows Server versions: Server 2012, 2012R2, Standard, Enterprise Foundation and Data Center versions along with 2012 Essentials (SBS) and , 2012 Storage Server; Server 2016, Server 2019 & Server 2022.

2016, Standard, Enterprise Foundation and Data Center versions along with 2016 Essentials (SBS) and , 2016 Storage Server. We currently do not have any clients running the data center or Essentials versions of 2012R2, 2016, 2019 or 2022. We currently do not have any clients running any 2022 Servers.

## *VMWare: (4.6)*

One of our clients has a VMWare cluster in place consisting of three VMware hosts that support 36 individual Windows and UNIX servers. It is configured in an auto fail over mode to support the failure of one of the host machines. The backup solution in place for this client is based upon NetVault software. A single VMWare Host supporting three windows servers has been recently configured and deployed and for a client in Wisconsin. Other clients have a single VM ware host machines similar to your current CCOC server environment.

## *Veeam Back-Up services: (4.7)*

The research and vetting of the Veeam product as a recommended solution in conjunction with VMWare was completed in 2014 and is still recommended in 2021. This product has been recommended and installed at several Clients. Multiple clients are using the product as part of their backup and security processes. .

## *Network Support Services: (4.8)*

Network support maintains all network software, hardware and infrastructure, including servers, switches, VPN, backup systems, and firewalls. They are also accountable for all network based services, such as email configuration and management in Office 365. They will assist CCOC with: Network Design and Implementation; Local Area Network (LAN) Support; Wide Area Network (WAN) Support; Virtual Private Network (VPN) Support; Routing and Communications issues; Wireless Network support; and Remote Access Services as required.

## *Server Administration: (4.9)*

Server administration maintains all servers and server based processes. This includes Domain Name System (DNS) servers, VMWare Servers and Windows based servers. Server services and processes consist of network authentication through one or more methods including Active Directory, network shares, network resources, file management, user profiles, and security issues as related to any server OS. It may also include more advanced services such as those related to databases (SQL), storage or content management systems, specialized proprietary services, and other industry-specific server-based applications.

## *Office 365: (4.10)*

eGroupTech is an authorized Microsoft Partner and reseller of Office 365 services. We currently support multiple clients on Hosted Exchange since 2010. Prior to Office 365 we have supported and continue to support multiple clients on other hosted exchange services. eGroupTech currently supports various Office 365 versions from 2018 through 2021.

## *eGroupTech - Overview (4.11)*

eGroupTech was Founded in 2002 to address the growing need for Technology Strategy and Technology Management within the Small - Medium Business market segment (SMB). The knowledge gained by utilizing technology to continuously improve business processes resulted in the formation of a company that understands and has developed the critical processes necessary to support the core technology and business processes for its clients.

eGroupTech is the outsourced technology company continuing to provide Managed Services as a MSP organization as well as standalone services for technical assistance, network support, training and programming services for our current clients.

eGroupTech has a trained and tenured chief technologist with over 40 years of experience. We are extremely effective with staying ahead of the technology curve to keep our client base running efficiently and effectively.

Our vision: Sustain a *"State of Excellence"* in our customer relationships, technical and business knowledge, products, services and support.

Our primary mission is:

- *“The Fusion of People, Processes and Technology"* within your business providing a sustained competitive advantage
- Provide business process and technology solutions to organizations that are cost effective, practical and add real value
- Partner of choice for all of your technology requirements from contract CIO/CTO services to desktop support
- Offer consulting, hardware and software products at competitive prices coupled with support contracts and training options designed to meet your company's needs
- Strive to be on the leading edge of technological knowledge by maintaining a staff of motivated, experienced, and highly trained employees working together collaboratively
- Committed to building and maintaining long term client relationships based upon service excellence and real solutions

Our organization supports the following values:

- Make and keep our commitments to customers, colleagues, the company and ourselves
- Show respect for others and ourselves by being open, honest, truthful and by resolving conflict
- Behave in an ethical, legal, fair and balanced manner
- Contribute to the growth and prosperity of our company through individual, team and total company effort
- Continuously learn, encourage one another, celebrate, and do worthwhile, high quality work

eGroupTech is a drug free workplace.

# Requirements: (5.0)

## Notice of Intent to Bid: (5.1)

eGroupTech submitted the intent to bid on November 08, 2021 via e-mail. Receipt was confirmed by the CCOC Exec Director John Dew.

## Format & Copies: (5.2)

eGroupTech submitted a complete electronic response to the CCOC RFP on November 23, 2021 via e-mail.

## The Proposal Shall be Signed: (5.3)

Please refer to section 5.4.1 below and the proposal cover page.

## Responses – Shall Include- Submission Information: (5.4)

Reference section 5.4.1 to 5.4.6 below:

### Authorizations: (5.4.1)

eGroupTech's respondent to the CCOC RFQ is:

Kenneth Baker, CM – President and Chief Technologist
2441 Monticello Drive.
Tallahassee, FL. 32303
V: 850-894-6400
kbaker@egrouptech.com
www.egrouptech.com
Respectfully Submitted:

Kenneth R Baker

## Qualifications, Certifications - Resumes: (5.4.2)

Reference section 5.4.2.1 to 5.4.2.3 below:

### Qualifications: (5.4.2.1)

eGroupTech as a corporation and Ken Baker as the President and Chief Technologist supports the following Core Technologies as they relate to client support:

**MSP:** eGroupTech changed its business model to become a MSP in 2014 and on boarded our first Managed Services Client. Today 90% of eGroupTech's clients prefer the MSP environment over the break fix model.

**Enterprise Server Based Applications:** Microsoft Server up to and including the current version 2022; Microsoft Exchange Server 2012, 2016 & 2019; Office 365 Hosted Exchange and other Hosted Exchange services; VM Ware ESX & ESXI; IBM-Lotus Domino / Notes; MaaS360 MDM, Document Imaging & Document Management systems NAS: OS- Qnap, Windows 2016 , 2019 storage server.

**Desktop Software and Applications:** Windows 10, 8.1 8 and 7; Microsoft Office 2021, 2019, and 2016, ; Corel Office; The Adobe Product Family; Graphics Applications, Various vertical market and functional applications and all of the various levels of Office 365 along with their related software and services.

**IT Software Support Applications:** Network and cloud based Antivirus Applications; Network and cloud based Workstation Anti Spy Ware / Ad Ware Applications; Spam and e-mail filtering software; and Network Security Applications

**Enterprise Installation & Support Services:** Cloud based Enterprise / workgroup backup solutions; Local Enterprise / workgroup backup solutions; High availability servers and clustering; Storage redundancy solutions; NAS & SAN storage devices; Server conversion and migration; Server consolidation, replacement or updates, Server Virtualization, Server migration to cloud.

**e-Commerce Services:** Internet and E-commerce Strategy; Web Site Design and Implementation; Web Hosting and Management; Corporate e-mail domains and identity; Internet e-mail configuration

### Certifications: (5.4.2.2)

**eGroupTech - Vendor Certifications / Relationships:** We are an Authorized Microsoft Partner and Office 365 reseller, a Veeam Pro Partner, Connect Wise Partner, Dell Authorized reseller, Lenovo Authorized Reseller and maintain several software partnerships.

## Resumes: (5.4.2.3)

Ken Baker C.M is a certified professional manager with extensive project management experience as it relates to technology strategy, planning, implementation and deployment. Ken holds a: Master's Degree in the Management of Technology from the University of Miami; A Bachelor's Degree in Business management and industrial supervision from Purdue University as well as Associates Degrees for Aviation Maintenance Technology and General Flight Technology.

The use of technology to improve business has been a lifelong experience, Various positions along his career path starting from the beginning are: industrial engineer; divisional budget planner, Corporate Manager of Planning Services, Network Administrator, Program budget planner for new product development, Quality manager for Business Systems, Senior Technical Engineer, Vice President of Technology, President and Chief Technologist. All experiences along the way have contributed to the successful organization that is eGroupTech.

Our customer focused and quality oriented back ground stems from being formally trained in the Total Quality Management TQM programs while working for a governmental contractor. Since 1992 our involvement on the Board of Directors for the Florida Sterling Council has provided a business management model that promotes performance excellence. Parts of the criteria from the model are used within our strategic planning and guidance for the clients of eGroupTech.

## Capabilities: (5.4.3)

eGroupTech clients rely on their technology to just work when they need it. It is our objective to help every client develop a technology strategy and plan based upon business objectives and processes. Our MSP services provide a going evaluation of your systems and processes ensuring that we continue to deliver the right services in the format that suits your organization and employees' preferences. After all, it is not just about IT but the integration of "People, Processes, and Technology" resulting in your organization becoming more efficient and effective.

Managed Services helps your employees be more efficient. It makes the end user technical support decisions easy. The employees no longer have to try and solve the issues themselves and worry about the resultant IT bill that the organization will get. The budgeting process is easy, the organization pays the monthly MSP invoice and the only other costs are hardware and software according to the IT operations plan.

eGroupTech has the network, desktop, laptop, server, tablet and smart device knowledge to support CCOC end user environments. We have developed a set of core competencies as a MSP to manage, maintain monitor and update your server, laptop and infrastructure environment so CCOC will have less interruptions in their day to day activities.

eGroupTech has a depth of knowledge that can only be accumulated by the been there done that level of hands on experience.

CCOC has a choice to select a vendor that will just show up when you call them (or have to call them multiple times) conversely, you select one that is proactive and will provide all of the services listed in the scope of services in this RFP within the SLA timeframes stated.

## ***References: (5.4.4)***

The references listed below represent a few medium to large multi user networks. Managed Services and technical support services for these clients consist of the following:

- Network infrastructures ranging from simple interfaces to complex networks with dedicated security and access control devices.
- On site and cloud server environments running windows, UNIX and VMWare. Most have multiple in house servers. Some run cloud based services.
- One or more dedicated backup processes that utilize an on-site NAS and an Off-site process for disaster recovery.
- Workstations in the environments consist of PC - MAC desktops and laptops. Mobile devices along with I-pads, I-phones, Android and Windows based tablets and smart phones are supported and integrated into the business systems.
- Cloud based services consist of: Office 365; other Hosted Exchange services, in-bound and outbound e-mail filtering, anti-spam; anti-virus solutions; anti-mal ware and other security solutions.
- One client runs a Mobile Device Management (MDM) platform that secures workplace content and data on company owned and BYOD devices. Remote wipe of the company data on any lost or stolen smart phone or tablet is simple.

Skandia Window Fashions
Hilmar Skagfield - President
V 850-878-1144 Ext 2102
Gil Martel – Director IT
V 850-878-1144 Ext 2104

Florida Sterling Council
Dione Geiger - President
V 850-922-5316

Champion Auto Sales
Jay Jubran
V 850-508-8119

## Monthly Managed Services Fee & Rates: (5.4.5)

eGroupTech Managed Services Provider (MSP) monthly fixed fee schedule for CCOC

| Service | Quantity Year 1 | Quantity Year 2,3 | Notes |
|---|---|---|---|
| Network Infrastructure | 1 ea. | 1 ea. | Production Network – 1ea Comcast Router, 1ea Cisco RV042G Router, 3ea TP-Link TL-SG1024DE switches and 1ea Ubiquity Wireless point |
| PC Management – Desktop / Laptop - Support | 10 / 10 | 10 / 10 | As indicated on the CCOC RFP diagrams |
| Server Management | 2 | 2 | One on site – Dell EMC R640 & PowerEdge R510 servers |
| NAS | 1 | 1 | WD RX4100 NAS |
| E-mail Admin and management and administration including Virus and Filtering software | Per user + Generic Accounts | Per user + Generic Accounts | |
| Standard PC App(s) | All | All | Office 365, Adobe, QuickBooks – per standardized list |
| Backup & Backup Monitoring | All | All | All Servers and laptops identified above and Off Site data |
| Wireless Network Management | 1 | 1 | Manage Access point |
| Network & Local Printers | All | All | Kyocera3051i – Local printers – Add drivers and connectivity |
| Network and local scanners | All | All | |
| IT Re - Assessment | 1 | 0 | Complete report Year 1<br>Updates included in additional years as part of MSP $ |
| Continued consulting on governance and Governance Plan | 1 | 0 | As necessary: any Updates included in Year 2/3 as part of MSP $ |
| Consulting on Strategic Planning and IT Strategic Plan | 1 | 0 | Additional 3 year Plan completed Year 1 Updates included in Year 2/3 as part of MSP $ |
| Backup Assessment and Backup Plan | 1 | 0 | Plan updated Year 1<br>Updates included in Year 2 as part of MSP $ |
| Security Threat Assessment | 1 | 0 | Assessment completed Year 1<br>Updates included in Year 2 as part of MSP $ |
| Security Consulting and a Security Plan | 1 | 0 | Plan completed Year 1<br>Updates included in Year 2 as part of MSP $ |
| CIO Services | 1 | 1 | Include in both years as part of the MSP $ |
| | $3175 | $2875 | |

There is not a onetime MSP Set up fee, as the use of the RMM system AV software and all of its components will continue in use. eGroupTech will continue to furnish work from home / remote access to CCOC's desktop computers for designated employees as part of the RFP at no additional costs.

Monthly IT MSP fees do not include the cost of new or replacement hardware, software, software as a service, cabling or other equipment that may be required to perform services under this agreement. CCOC may procure equipment independently or a quote can be furnished for new or replacement equipment. Sterling will pre-approve any software and equipment purchases. Purchases by eGroupTech will be billed separately at the end of the month or when the order is placed if the purchase price exceeds $500.

For the first 12 months of this proposal monthly costs are $3175. For annual extension months 13 through 36, the costs of the monthly support will be $2875 per month.

The current month's service invoice will be billed on or before the 1st business day of the current month net 15.

### Litigation: (5.4.6)

eGroupTech, Inc. has not been involved in any litigation during the past five (5) years involving the organization, the respondent or any person(s) listed in this RFQ relating to professional services, including a summary of the disposition of such matter or matters. eGroupTech, Inc. has not had any grievances filed within the past five (5) years against the organization, the respondent or any person(s) listed in the response with any regulatory or judicial body, including a summary of the disposition of such matter or matters.

## Contract: (9.0)

The following eGroupTech documents are provided as attachments to the RFP submission. They are confidential documents and will be part of the contractual arrangement. They may NOT be published on the CCOC Web site as part of the response to this RFP.

Help Desk Process and procedures – Furnished to CCOC if Contract is awarded. – Confidential document

## Appendices:

### Appendix A: List of Hardware and Software Covered by MSP Service

This appendix lists the equipment and software that will be supported under the unlimited on site and remote technical assistance (MSP) plan as defined in this response to RFP. Exclusions are also listed.

The data is taken from the two CCOC diagrams listed in the RFP:

1) FLCCOC Ethernet Lan Diagram and
2) FCCOC topical network diagram.

The unlimited service covers current hardware and software and the replacement of those items:

1) i.e. A laptop or desktop breaks and a new one is ordered – Labor for the replacement device is covered as long as the replaced device is taken out of service.
2) Updating Software (labor) – i.e. Updating Office 365 to a newer version is covered. Updating QuickBooks to a newer version is covered.
3) Labor for the replacement of components is included but the cost of the replacement hardware, software, or consumable is a CCOC cost: i.e. CCOC will purchase the replacement batteries for the APC units, and eGroupTech will install under the MSP contract.

E1) Specifically Included Equipment:

- Ten (10) windows desktops – On Site
- Ten (10) windows Laptops - On Site / Off Site / Work from home
- Dual & Triple monitor display support on devices with more than one monitor
- One (1) Dell EMC R640 Server – On Site
- One (1) Dell power edge R510 server – On Site
- One (1) WD RX 4100 NAS – On Site
- Three (3) TP-Link TL-SG1024DE 24 port Gigabit switch(s)
- One (1) Cisco SB Router – RV042G
- Two (2) APC Back up Power supply units – data center closet
- One (1) Unify wireless access point
- All Desktop Back up power supply units (if currently installed)
- LAN wiring and patch cables – punch downs or replacement patch cables
- Any mobile devices (company owned or BYOD) needing access to the wireless access point or e-mail configuration
- CCOC has 15 days after contract award to correct this list (if necessary).

E2) Specifically Excluded Equipment:

- Kyocera 3051ci Printer – Warranty and replacement issues are the responsibility of the printer vendor.
- PRINTER SCANNER NOTE(s):
    - Installation of printer drivers and basic printing / troubleshooting printer issues is covered as part of CCOC's Managed Services.
    - Installation of Scan drivers, Scanning and Printer Name & Address book and scanning users is covered as part of CCOC's Managed Services.
    - Vendor coordination for major printer issues is included (note SLA metrics do not apply because the schedule and response to physical printer issues are based upon the Printer vendors' response.
- Comcast Business Gateway – (cable modem / router)

- COMCAST NOTE(s):
    - Physical failure of the device is the responsibility of Comcast.
    - Vendor coordination of the replacement and unique configuration relative to CCOC's WAN/LAN network is covered as part of CCOC's Managed Services.
    - Vendor coordination for ISP / cable modem- router issues is included (note SLA metrics do not apply because the schedule and response to physical modem / router issues are based upon Comcast's vendor Response
    - eGroupTech must be added an authorized account contact and other account contacts should be reviewed at that time.
- Xblue X16 Digital phone system and Grace Digital Audio system
- Actual phones for system above

E3) New – Additional Hardware:

New hardware added to the list of software for CCOC's use can be requested, procured and installed as a Project (request for additional services). Fees for such additional services or out of scope work will be presented as an authorized Change Authorization Order (CAO), which will also provide a description of the changed or additional service(s) being requested. Once a CAO is signed by both parties, it will be incorporated into the Agreement and have the same legal effect as the SOW or contract that is incorporated into the IT Master Services Agreement. The CAO will also provide a projection of the monthly Managed Services cost increase once the hardware request is implemented. The CAO will be billed on a separate invoice on a monthly basis. All / any CAO's will become a requirement in any future RFP that CCOC issues.

S1) Specifically Included Software - Workstations:

- Office 365
- Office 365 Hosted Exchange Services
- QuickBooks
- Web Root AV program
- Last Pass
- Adobe Acrobat
- Adobe Reader
- Adobe Shockwave
- Apple iTunes
- Google Chrome Browser
- Mozilla Firefox Browser
- Oracle Java
- PDF Creator (or similar)
- 7-Zip (or similar)
- Snagit Application
- Notepad++
- Windows, VLC Media Player (or similar)
- CCOC has 15 days after contract award to correct this list (if necessary).

S2) Specifically Included Software - Servers:

- Microsoft Server (any current or new version)
- VMWare (any current or new version)
- Veeam Backup software (any current or new version)

S3) Specifically Excluded Software:

- Any software or Software As a service (SAS) that has not been disclosed in the original RFP or added to the specifically included software list above within the 15 day limit after contract award.

S4) New Software:

New software for CCOC's use can be requested, procured and installed as a Project (request for additional services). Fees for such additional services or out of scope work will be presented as an authorized Change Authorization Order (CAO), which will also provide a description of the changed or additional service(s) being requested. Once a CAO is signed by both parties, it will be incorporated into the Agreement and have the same legal effect as the SOW or contract that is incorporated into the eGroupTech's IT Master Services Agreement. The CAO will also provide a projection of the monthly Managed Services cost increase once the software request is implemented.

## *Appendix B: Summary of MSP Tasks, Activities, List of Services*

B-1: Desktop Support - Managed workstation tasks

- New user adds removes and changes to workstations including access to devices as necessary
- Workstation initial build and full configuration through delivery to end user
- Install and troubleshoot workstations including workstation OS, device drivers and connectivity
- Install and troubleshoot workstation applications. Support and troubleshoot all standard software including Adobe products, MS Office, and other software as determined by the list of specifically includes software – workstation in Appendix A-S1
- Provide emergency remote and on site break / fix operations for workstations, laptops and tablets
- Manage printer issues, print drivers, printer installations and printer driver updates
- Manage scanning issues, scan drivers, scanner installations and scan driver updates
- Manage workstation connectivity including drive mappings, back up connections and other access issues to the network or applications that are network based or cloud based.
- Manage all aspects and Admin functions for workstations
- Manage user credentials / security and provide account lockout and password reset services as designated
- Create, modify or change CCOC documentation for workstations and desktop applications, in support of corporate IT best practices
- Manage all aspects of the RMM Managed Workstation Application for all desktops

- Provide patches and updates as necessary for all workstations
- Be responsible for IT asset and inventory management as part of the Managed Workstation Application. Includes hardware and software inventories.
- Installation, monitoring and verification of workstation data back-up including logs / alert monitoring as requested

B-2: Server Support - Managed server – Active Directory (AD) tasks

- New user adds removes and changes to servers / AD including access to resources as necessary
- Server initial build and full configuration through delivery to end user
- Install and troubleshoot servers including OS, device drivers and connectivity
- Install and troubleshoot server applications. Support and troubleshoot all standard server software as determined by the list of specifically included server software – workstation in Appendix A-S2
- Provide emergency remote and on site break / fix operations for onsite servers – Host vendor responsible for VPS server
- Manage server connectivity including security for drive mappings, back up connections and other access issues to the network or applications.
- Manage all aspects and Server Admin, maintenance and AD services.
- Manage user credentials / security and provide account lockout and password reset services as designated
- Create, modify or change CCOC documentation for servers in support of corporate IT best practices
- Manage all aspects of the Managed Server Application for all Servers
- Be responsible for IT asset and inventory management as part of the Managed Workstation Application. Includes hardware and software inventories.
- Installation, monitoring and verification of server data back-up including logs / alert monitoring as requested

B3: Network Support - Managed network tasks

- New user adds removes and changes including access to devices as necessary
- Router or switch initial build and full configuration through delivery to end user
- Install and troubleshoot Router and switches and connectivity
- Provide emergency remote and on site break / fix operations for Router and switches
- Manage network based printer issues, print drivers, printer installations and printer driver updates
- Manage network based scanning issues, scan drivers, scanner installations and scan driver updates
- Manage network connectivity providing drive mappings, back up connections and other access issues to the network or applications that are network based or cloud based
- Manage all aspects and Admin functions of the network including AD
- Manage all aspects of any local Wireless network devices including SSID's and passwords as designated. Includes any new or replacement installations of devices,

- Create, modify or change CCOC documentation for the network infrastructure in support of corporate IT best practices
- Work with a designated individual as necessary for coordination of information and technical knowledge
- Installation, monitoring and verification of network devices including back-up configurations, logs / alert monitoring as requested

## Appendix C: Proposed Schedule of Activities and Timeline

The data in this section will become a live schedule. This outline is not intended to be all inclusive at this point in time. Dates for projects and assessments are dependent upon CCOC and eGroupTech resources being available at the same time to do the work involved in the processes. The timing and sequence of the projects are based upon eGroupTech's recommendations. A final schedule will be set once priorities are worked out with CCOC.

Defined as days / weeks / months after contract award:

Day 15:

- Re run basic reports from the RMM tool as the start of the CCOC IT assessment / reassessment

Day 20

- Update and re-Issue eGroupTech Transition document including Help Desk Contact information. (Primarily for employees in the last year)

Week 2 – Review Off-Site BU process and get CCOC on owned account

Week 4

- Start Security Threat Assessment

Week 5

Week 6

- Back up Assessment started and updated to current processes

Week 7

Week 8

- Revisit policy development

Week 9

Week10

Week 11

Week 12
Month 2

- Start IT Governance and strategic planning process

Month 4

- Security Assessment planning complete

Month 5
Month 6
Month 7

Month8

- Finish Policy Development

Month9

- Finish IT Governance and strategic planning process

Month10

Month 11

Month12