Center for Computer Resources, LLC

Description of the Managed IT Services System

SOC 2 Type 1 Report

As of December 31, 2019

Cohen & Co

cohencpa.com

CENTER FOR COMPUTER RESOURCES, LLC.

DESCRIPTION OF THE MANAGED IT SERVICES SYSTEM
SOC 2 TYPE 1 REPORT

TABLE OF CONTENTS

SECTION I

Independent Service Auditors' Report

Cohen & Co®

Independent Service Auditor's Report on Center for Computer Resources, LLC.'s
Description of the Managed IT Services System and the Suitability of the Design of Controls

Management
Center for Computer Resources

Scope

We have examined Center for Computer Resources' accompanying description of its Managed IT Services system found in Section 3 titled Description of the Managed IT Services System as of December 31, 2019 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of December 31, 2019, to provide reasonable assurance that Center for Computer Resources' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria*). The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Center for Computer Resources, to achieve Center for Computer Resources' service commitments and system requirements based on the applicable trust services criteria. The description presents Center for Computer Resources' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Center for Computer Resources' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Center for Computer Resources uses a subservice organization to for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Center for Computer Resources, to achieve Center for Computer Resources' service commitments and system requirements based on the applicable trust services criteria. The description presents Center for Computer Resources' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Center for Computer Resources' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Center for Computer Resources is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Center for Computer Resources' service commitments and system requirements were achieved. In Section II, Center for Computer Resources has provided the accompanying assertion titled "Assertion of the Management of Center for Computing Resources, LLC". (assertion) about the description and the suitability of the design of controls stated therein. Center for Computer Resources, LLC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design of controls involves -

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects -

a. the description presents Center for Computer Resources' Managed IT Services System that was designed and implemented as of December 31, 2019, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of December 31, 2019, to provide reasonable assurance that Center for Computer Resources' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Center for Computer Resources' controls as of that date.

Restricted Use

This report is intended solely for the information and use of Center for Computer Resources; user entities of Center for Computer Resources' managed IT services system as of December 31, 2019; business partners of Center for Computer Resources' subject to risks arising from interactions with the managed IT services system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Cohen & Company Ltd.

Detroit, Michigan
June 18, 2020

SECTION II

Assertion of the Management of Center for Computer Resources, LLC.

CCR
Center for Computer Resources
36333 Mound Road • Suite C • Sterling Heights • Michigan • 48310
Phone: 248.284.7100 • Fax: 248.284.7101 • E-Mail: servicedesk@ccr1.com
www.ccr1.com

Assertion of the Management of Center for Computer Resources, LLC

We have prepared the accompanying description of Center for Computer Resources, LLC's Managed IT Services System titled Center for Computer Resources, LLC Description of the Managed IT Services System as of December 31, 2019 (description), based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Managed IT Services System that may be useful when assessing the risks arising from interactions with Center for Computer Resources, LLC's system, particularly information about system controls that Center for Computer Resources, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

As indicated in the description, Center for Computer Resources, LLC uses a third party data center for hosting customer servers, as well as its own servers (subservice organization). The description includes only the applicable trust services criteria and related controls of Center for Computer Resources, LLC and excludes the applicable trust services criteria and related controls of the subservice organizations. The description also indicates that certain applicable trust services criteria specified in the description can be met only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Center for Computer Resources, to achieve Center for Computer Resources' service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that

1) The description presents Center for Computer Resources, LLC's Managed IT Services System that was designed and implemented as of December 31, 2019, in accordance with the description criteria.

2) The controls stated in the description were suitably designed as of December 31, 2019, to provide reasonable assurance that Center for Computer Resources, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Center for Computer Resources' controls as of December 31, 2019.

CENTER FOR COMPUTER RESOURCES, LLC

By: _____

Title: CTO/PARTNER

Date: 6/18/20

SECTION III

Description of the Managed IT Services System

A. Center for Computer Resources and Managed IT Services Overview

The Center for Computer Resources (CCR or the Company) was founded in 1981 to help small businesses in southeastern Michigan get the most out of their business technology. CCR is headquartered in Sterling Heights, Michigan with branches in Traverse City, Michigan and Petoskey, Michigan. With almost four decades in the business, CCR has extensive experience in transitioning user entities from outdated systems to current technologies, as well as maintaining current systems. With a help desk, investment in sophisticated tools, and a focus on security, CCR is able to provide enterprise level information technology services that allow its clients to focus on their businesses.

CCR provides technical services to approximately 250 small and medium size companies, representing a wide variety of industries, including healthcare, manufacturing, professional and business services, and retail. The clients range in technology size from 3 computers to 275 computers, including desktops, laptops, and servers.

The Managed IT Services System offers the following services, which are described in more detail in the following section:

- Managed Network Solutions
- Managed Servers and Desktops
- Email Protection
- Managed Firewall
- Backup and Rapid Recovery
- CCaRe Hosting Plan

B. Managed IT Services System Boundaries

The offerings of CCR's Managed IT Services System are named "CCaRe" and consist of various service level offerings such as managed network solutions, managed servers and desktops, email protection, managed firewalls, internet optimization and monitoring, back-up and recovery, and cloud hosting of IT resources.

Managed Network Solutions

CCaRe is intended to reduce costs of hardware ownership and software upgrades, and to increase security by centralizing access to data. System updates, upgrades, and patches are applied and pushed to remote locations. CCR systems monitor the base operating system, email servers, database servers, remote equipment and backup processes. Key system thresholds are monitored and alerts are sent to a dedicated service ticket system for resolution of identified issues.

Depending on user entity selection, managed services can include: hardware and software; next business day hardware replacement; real-time updates for security, spyware and virus content to block new internet threats; software version upgrades and firmware upgrades; comprehensive security gateway; real-time limited gateway, anti-virus, anti-spyware; intrusion prevention; deep packet inspection firewall; centralized management, monitoring and reporting; real-time monitoring of network usage; and detailed historical reporting of network availability, blocked threats and internet use.

B. Managed IT Services System Boundaries (Continued)

Managed Servers and Desktops

CCR systems monitor clients' base operating systems, email servers, database servers, and backup processes. Key system thresholds are monitored and alerts are sent to a dedicated service ticket system for any issue that may arise. A dedicated team of system engineers troubleshoot, resolve problems, and proactively perform necessary preventative maintenance on client servers. Various hardware and software inventory reports are available so clients are able to understand the assets they own. Operating system patches can also be applied based upon the plan option selected.

Desktop plans provide a comprehensive preventative maintenance regiment for desktop and laptop computers, keeping them secure and operating at peak levels of performance. All Desktop plans include CCaRe email protection and advanced SPAM filtering, which is intended to block 99% of SPAM. Remote desktop and laptop support tools allow help desk engineers to remotely control and share client devices.

E-mail Protection

Email Protection provides comprehensive email security and management. It is configured to block spam, viruses, and email attacks, and provides message management, and policy enforcement capabilities.

The Email Protection spam filter scans every email sent to client accounts, verifying the legitimacy of the email, and determining the likelihood of the email containing spam. Clients receive a daily quarantine email summary informing the client of suspicious email. Clients then select the emails they want in their inbox. The spam filter service is intended to capture 99% of unwanted email.

Directory harvest and denial of service attacks are stopped by exclusive Sender Behavior Analysis. Spam, viruses, and other email threats are stopped before reaching client networks. White and black-lists are maintained for both senders and IP addresses. Email Protection provides protection from a variety of increasingly sophisticated attacks from hackers, spammers, and phishers.

Email Protection also includes disaster recovery and failover. This prevents email loss during server or internet outages by automatically spooling incoming messages, then unspooling and delivering them when servers are restored. Messages are never lost or bounced back to the sender.

Managed Firewall

CCaRe Managed Firewall provides a fully managed firewall and security solution to protect business networks. This service provides 24x7x365 monitoring and proactive management. Firewalls are configured to allow "good" traffic in and to keep "bad" traffic out. Firewalls are continuously updated to support changing business requirements.

B. Managed IT Services System Boundaries (Continued)

Managed Firewall (continued)

Managed Firewall includes the following services:

- Real-time, limited gateway anti-virus, anti-spyware, and intrusion prevention.
- Deep packet inspection firewall.
- Configuration changes, firewall policy management, and backup of all devices.
- Real-time monitoring of network usage.
- Detailed historical reporting of network availability, blocked threats, and internet use.
- Filtering to control access to unwanted web content.
- Flexibility to filter questionable or inappropriate content by category.
- Next business day hardware replacement.
- Real-time updates for security, spyware, and virus content to block new internet threats.
- Software version and firmware upgrades.

Backup and Recovery

CCaRe Backup and Rapid Recovery (BaRR) provides an integrated approach to business systems continuity, which enables businesses to quickly recover systems and data when systems malfunction, software becomes corrupted, viruses spread, or natural disasters occur. CCR's recovery system includes turnkey appliances and proprietary technologies that provide rapid recovery for virtually any system back to a desired point in time.

The Backup and Rapid Recovery solution features the housing and maintenance of an offsite storage shuttle drive. BaRR has the capability to prepare a hot swap hard disk drive that includes a complete image of the entire server infrastructure. The solution includes two hot swap hard disk drives which allow for off-site storage as well as weekly rotation. These hot swap disk drives are formatted to facilitate daily incremental backups and will contain a full system image. Backup is fully automated, with no system downtime required. Performance is monitored real time and failures are sent to a dedicated service ticket system for resolution. Complete data protection is provided: all programs, settings, configuration, systems, and user data.

Cloud Hosting Services

With CCaRe Cloud Hosting Services, CCR manages and hosts all of a client's IT needs. User entity applications and data reside on CCR-owned servers. Servers are physically located at a third party subservice organization, and accessed and serviced remotely. CCR monitors servers and remote equipment 7 days a week, 24 hours a day. CCR staff performs regular maintenance tasks to prevent difficulties and will respond whenever a problem occurs. CCR monitors the base operating system, email servers, database servers, firewall, backup processes, and alerts are sent to a dedicated service ticket system for resolution of identified issues. A team of system engineers troubleshoot, resolve problems, and proactively perform necessary preventative maintenance on the servers.

B. Managed IT Services System Boundaries (Continued)

Complementary User Entity Controls

The accompanying description of the Managed IT Services System includes control activities that comprise only a portion of the overall internal control for each user entity. It is not feasible for the trust services criteria related to this system to be solely achieved by Center for Computer Resources. The Managed IT Services System controls were designed with the assumption that certain controls would be in place and in operation at the user entity. User entity internal controls must be evaluated, taking into consideration Center for Computer Resources' controls, and their own internal controls. Center for Computer Resources, as a service organization, does not provide any assurance that the user entity has implemented proper user entity controls, and or that such controls are properly functioning.

This section describes some of the control considerations for the user entity, or "complementary user entity controls", which should be in operation at the user entity to complement the controls at Center for Computer Resources. User auditors and management should determine whether the user entity has established controls to ensure that the criteria within this report are met. The "complementary user entity controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by the user entity. There may be additional criteria and related controls that would be appropriate for the user entity that are not covered by this report.

Control Considerations for the User Entity:

1. The user entity is responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate, including access provided for temporary or contract users.
2. The user entity is responsible for user accounts that need to be added or removed due to employee termination or transfer of job responsibilities.
3. The user entity is responsible for securing the method to request and remove access to ensure that appropriate users are requesting access to systems.
4. The user entity is responsible for monitoring access to its systems, to insure that only authorized users are accessing them, and that any unauthorized access or security incidents are reported to CCR.
5. The user entity is responsible for ensuring the communications method utilized to connect to hosted servers are secure from internal and external threats.
6. The user entity is responsible for developing their own disaster recovery and business continuity plans to supplement the CCR services.

C. Use of Subservice Organization

The Company uses a subservice organization data center to provide its cloud hosting services. The controls performed by the subservice organization that relate to the security trust services criteria are not included in or covered by this report. Where applicable, and as part of its monitoring activities, the Company obtains a service organization controls report from the subservice organization in order for management to assess the adequacy of controls in place, and to assist with its risk assessment activities. The following trust services criteria applicable to the system can only be met if suitably designed and functioning controls at the subservice organization include:

Controls CCR Expects Subservice Organization has in Place	Trust Service Criteria Impacted
• System changes and incidents that affect internal and external users are communicated in a timely manner. • Formal processes are implemented for granting, modifying, revoking, and reviewing user access rights to system resources. • Access to system resources is restricted to authorized users. • Physical and logical access controls are properly implemented. • Proper firewalls and encryption technologies are in place to secure access and to conceal sensitive data. • Data backup and disaster recovery plans are in place and tested periodically. • A formal documented change management process is in place, reviewed periodically, and used for all changes.	**CC2.2, CC4.1, CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC7.2, CC7.3, CC7.4, CC7.5, and CC8.1**

The description presents CCR's system, its controls relevant to the security criteria, and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet the security trust services criteria. The description does not include any of the controls implemented at the subservice organization.

C. Relevant Aspects of CCR's Control Environment, Risk Assessment, Information and Communication, and Monitoring

Control activities related to the Company's applicable Trust Services Criteria are effected by the Company's management, and other personnel and are composed of four interrelated components:

- Control Environment
- Monitoring
- Risk Assessment
- Information and Communication

Control Environment

CCR's control environment reflects the overall attitude, awareness, and actions of CCR's management concerning the importance of internal control and its emphasis within the Company. The organizational structure, assignment of authority and responsibility, documentation of policies and procedures, and regular weekly, monthly, and quarterly meetings are the methods used to define, implement, and assure effective controls. The organizational structure of CCR facilitates the flow of information utilizing an "open door" communication policy. The owners hold oversight roles in the organization and are actively involved in the day-to-day operations of the Company.

Integrity and Ethical Values

Management is committed to maintaining the highest levels of ethics and integrity. Management endeavors to foster this culture by promoting cooperation, coordination, communication, and alignment of interest among management, employees, and clients. There is direct communication between each team and the owners on a daily basis conveying the message that integrity and ethical values cannot be compromised. Management continuously demonstrates, through words and actions, a commitment to high ethical standards. At CCR, each employee is responsible for the consequences of his or her actions. If an employee is unsure of the appropriate action, the employee can take advantage of the owners' open door policy and informal environment to raise the concern with management.

Documented organizational and employee policies are in place that communicate entity values and behavioral standards to personnel. Employees are required to complete a new hire orientation that includes training in the Company's policies and procedures. Employees are required to sign the employee handbook to confirm their understanding of and compliance with the policies.

All CCR employees are required to acknowledge and sign an Acceptable Use Agreement (AUA). Users are not given access to the CCR network until they have signed the AUA. The AUA details the permitted system uses, user activities, and the consequences of non-compliance. An AUA is a key activity for user awareness and administrative policing of system activities.

D. Relevant Aspects of CCR's Control Environment, Risk Assessment, Information and Communication, and Monitoring (Continued)

Integrity and Ethical Values (continued)

The agreement also provides employees with clear guidelines of the employee's role in protecting client information. Policies include safeguards for protecting confidential information. Access to confidential information is limited to CCR business use. The use of confidential information for any other purpose is a violation of policy. Annually, all employees recertify their acknowledgement of an agreement with the policies and practices of CCR by signing an Acceptable Use Agreement.

Management has made it clear that CCR will comply with all applicable laws and regulations. All managers and employees are expected to conduct business in accordance with the letter, spirit, and intent of all relevant laws and to not do anything that is illegal, dishonest, or unethical.

Risk Assessment Process

Management performs on-going risk assessment to identify and manage risks that could affect the Company's ability to provide system security to user entities. As part of the on-going risk assessment process, management identifies changes to IT risk based on new applications and infrastructure, significant changes to applications and infrastructure, new environmental security risks, changes to regulations and standards, and changes to user requirements as identified in service level agreements and other documents.

Subservice organizations are assessed for risk at a high level. As part of this assessment, management will review available subservice organizations' SOC reports for user control considerations and reported exceptions. Weekly executive meetings are held to discuss new developments and the impact they have on the Company's risk profile. Management will implement changes to security processes as deemed necessary in response to changing risk. The Security Officer updates the security policy to reflect changes in policy and operating procedures. Senior management considers developments in technology and the impact of applicable laws or regulations on the entity's security policies. Management monitors the impact of emerging technologies, client requirements, and competitive activities by attending seminars and maintaining communication with other interested users.

Management evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process. As business needs dictate, the organizational structure is modified to help meet changing commitments and requirements.

Monitoring of Controls

Intrusion detection systems and other tools are used to identify, log, and report potential security breaches and other incidents. Monitoring systems are integrated to CCR's ticketing system, ConnectWise. The system will generate a ticket when a potential issue is detected and, depending on the issue, will notify the responsible network administrator via email. All incidents are tracked by management until resolved. The ConnectWise system provides "dashboards" for management monitoring of open tickets. Individuals assigned to resolving tickets document the final resolution on the ticket.

D. Relevant Aspects of CCR's Control Environment, Risk Assessment, Information and Communication, and Monitoring (Continued)

Monitoring of Controls (continued)

The Incident Response Plan includes a defined incident escalation process and notification mechanisms. When a significant incident is detected or reported, a defined incident management process is initiated and the Director of Professional Services is notified. The Director will lead the effort to perform the rest of the process. Corrective actions are implemented in accordance with the incident response plan.

The system monitoring tools scan all servers and computers, and identify updates, upgrades, and patches needed. The Director of Professional Services and the system administrator will review the list and decide which ones will be installed. Network performance and other reports are reviewed by management. Issues are brought to management meetings for discussion and inclusion in the on-going risk assessment.

Information and Communication

Various direct and indirect methods of communication are implemented by management to ensure employees understand procedures, standards, and guidelines developed to define their individual roles and responsibilities. Examples of these methods include orientation and training for new employees, emails, ongoing training, distribution of changes to policies and procedures, and on-the-job training.

Employees have daily access to the owners of CCR, who hold regular staff meetings at which employee feedback and suggestions are encouraged. The owners and management team regularly discuss internal control procedures with employees through staff meetings and on-the-job training and coaching. Management consistently stresses the importance of adhering to established control procedures and solicits recommendations from employees on how controls might be enhanced. Periodic IT staff meetings are held to address system performance, availability, capacity, and security concerns and trends; findings are discussed at quarterly management meetings.

CCR has also implemented various methods of communication to support its customer base. Users are provided instructions for communicating system availability issues, potential security breaches, and other issues. Customers can call the help disk or can request service by submitting a service ticket in ConnectWise, via CCR's web-based portal. Customers are notified of ticket resolution via automated email. Authorized customer (user entity) administrators can access all tickets submitted by their company.

Mechanisms are in place to allow CCR to notify customers of potential or actual operational issues that could impact the customer. ConnectWise Manager provides the ability to develop multiple email distribution lists for communicating to customers. This allows CCR to tailor messages specifically to affected customers only. Customers can also opt in to receive SMS alerts via their cell phones.

Communications are supplemented by email and telephone as needed.

E. System Components

Infrastructure

CCR uses a third party subservice organization data center for its cloud hosting services. In addition to maintaining its own corporate infrastructure at the data center, CCR also uses the data center to host its user entities' hardware and software applications. The data center provides the physical rack, circuits, and internet access, and is responsible for physical security, power, and environmental protection. The Company expects that the subservice organization has implemented appropriate controls for these areas.

CCR's corporate and user entity computer equipment is located in a restricted area within the data center. All access into the secured area of the facility is controlled through electronic keycards assigned to authorized individuals. Individual equipment racks are secured by separate combination or mechanical locks.

CCR's information systems environment comprises the following:

- 9 host servers in an HP Blade Chassis rack mountable enclosure.
- Each blade server is equipped with dual X5550 quad core 2.66 GHz processors and 144 GB of RAM.
- DL580 has Quad 6 core E7-4807 CPU's – total of 8 Blades and 1 DL580.
- VMware Enterprise Edition is implemented for the virtual environment.
- Windows 2008 R2 is implemented for all production servers.
- A hypervisor firewall separates each client's server data, with no open ports.
- P4500 G2 28.8TB SAS Multi-Site SAN with (48) 600 GB 6G 15K LFF Dual-port ENT SAS HP LeftHand P4500 10.8TB SAS Virtualization SAN with:
  - Dual redundant, active-active storage controllers
  - (24) 450 GB 15K SAS disk drives
  - 4 GB RAM, redundant
  - Hot swap power supplies
  - 1,024 MB battery backed cache
  - Support for RAID 5, 6 and 10
- Dual redundant, active-active storage controllers(4) 1Gbit NIC
- EMC VNX5300
- Dual redundant controllers and power supplies
- 26 NL SAS 1.8TB drives
- 11 SAS 268GB drives
- 8 flash 100GB drives
- 38 TB Total in Raid 5 pool with 4 hot spares

Software

CCR uses ConnectWise Manage, a fully integrated professional services application housed at the data center, to manage all user entity related information, service requests, projects and system configurations. ConnectWise stores all user entity information, such as contact information, authorized personnel, escalation procedures, service tickets, server and infrastructure configuration, and user entity user names and passwords. ConnectWise provides the ticket-generation system, which is used for all user entity requests, complaints, and alerts generated from various monitoring systems. It provides various reporting mechanisms for outstanding tickets and cleared tickets. Tickets remain outstanding until properly resolved and cleared. ConnectWise Control (formerly called Screen Connect), provides encrypted transmission for remote access.

E. System Components (Continued)

Software (continued)

IT Glue is a cloud-based software that offers a structured way to document IT systems. IT Glue's software includes features to standardize documentation such as password management, device tracking, and asset inventory, allowing CCR staff to more efficiently access data. CCR uses IT Glue for on-boarding new customers, and is transitioning customer data currently on ConnectWise Manage to IT Glue. This is an on-going process. In the interim, key data is synched between the two systems. Google Authenticator provides multi-authentication for access to IT Glue.

LabTech is CCR's remote monitoring and management (RMM) software application. LabTech performs support and maintenance tasks remotely, manages backup and recovery, provides password and patch management functions, and continually monitors system components. LabTech is used to monitor all customer remote servers and computers, including hosted servers and CCR computers and laptops. LabTech monitors a wide variety of events, including event logs on remote servers, daily backup failures, equipment failures, offline, email down, antivirus updates, and preventive maintenance. LabTech integrates to the ConnectWise system, and identified events will generate a ticket in ConnectWise Manage for research and resolution. Bright Gauge is business intelligence software that uses data from ConnectWise Manage and LabTech to build customized reports to help manage and monitor the network and devices.

Two layers of SonicWALL firewall software protect the network from unauthorized external entry and are integrated with CCR's ConnectWise system. Unauthorized attempts are blocked and reported. Logic Monitor continually gathers information from SonicWALL and provides a dashboard for continual monitoring. In addition to reporting unauthorized entry attempts, Logic Monitor will also report on hardware status. Reportable events are transmitted to ConnectWise, which will generate a ticket for research and resolution. CCR has a global management systems (GMS) Firewall, which allows CCR to upgrade firmware for all firewalls from a centralized point.

Additional software used by CCR includes the following packages: Webroot provides anti-virus and malware protection; Exchange Defender filters email spam; Some user entities are on Reflexion, which provides email security, email archiving, and email encryption; AuthAnvil provides multi-authentication capability for both CCR employees and clients; and Entrust manages the encryption keys.

People

Positons involved in the operation and use of the system are:

- **Executive Management** – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.
- **Managed Services** – manages and protects users' information and system from unauthorized access and use.
- **Help Desk, Field Services, and Mobile Applications** – provides user entities with assistance, information, and guidance, as requested and in response to customer service requests, technical issues, and complaints. Develops mobile applications.
- **Finance And Administration** – provides financial and administrative support including human resources, accounting, purchasing, payroll, and marketing and communication.

E. System Components (Continued)

People (continued)

Management considers the competence and technical levels for particular jobs and translates required skills and knowledge into written job descriptions. Management assesses each job candidate to determine whether the candidate possesses the required level of competence to hold the position. Only those candidates holding industry specific certifications are considered for certain technical positions. New personnel are offered employment subject to reference validation. Technical candidates are subject to the approval of Director of Professional Services.

Personnel policies are documented. Significant policies are available to employees on the corporate intranet. Upon employment, employees are required to acknowledge receipt and understanding of employee policies.

New employees must also sign an Acceptable Use Agreement (AUA), signifying that they have read, understand, and will follow these policies. The agreement covers expected and prohibited behaviors as they relate to security. Each year, employees must reconfirm their understanding of, and compliance with, the information security policies by acknowledging the AUA.

The entity has written job descriptions specifying the responsibilities for key job positions. Periodic performance appraisals are performed by supervisors. Regularly scheduled meetings are held to discuss special requests, operational performance, technology issues, and status of projects in process.

Data

CCR does not process transactions or data for hosted and managed user entities on user entity software. CCR does not identify, record, process, summarize, or report transactions for client organizations. CCR manages the IT resources necessary to allow user entities to process their own transactions.

CCR uses the ConnectWise Manage software, which is a fully integrated package that uses one database to share information for all user entity functions. User entities enter their own service ticket information by logging into CCR servers remotely using individually assigned user IDs and passwords. Remote access is provided by an SSL certified user entity portal. Only authorized users have access to company specific data.

Onboarding of new customers is a defined process, designed to capture the customer data needed to properly service customers. Templates are used to facilitate collection of information, including primary contacts, authorized individuals, critical applications, ISP, software, passwords, computer equipment and devices, etc. This data is entered into IT Glue and used for project implementation and ongoing customer service. Authorized access to the data requires multi-authentication using Google Authenticator.

Any change to data in ConnectWise is logged, along with user name and date. System changes are logged by the operating system and auditing is enabled on the Windows servers.

E. System Components (Continued)

Data (continued)

Infrastructure data from the primary and supporting systems are used to facilitate CCR monitoring and resolution activities. Specific data includes, but is not limited to, the following.

- Activity logs of access attempts, including denied access attempts.
- Alert notifications and monitoring reports.
- Activity logs from firewalls, routers, and switches.
- Alert notifications of failed data backups.
- Intrusion detection reports.
- Incidents and issue reports documented within the automated ticketing system.
- Network performance, system availability, and security incident statistics reports.

Control Activities

Physical Security Procedures

CCR is located in an office building with a security system to restrict access after normal working hours. Doors are always locked and passkeys are required for entry to the offices when an attendant is not on duty at the front desk. Visitors must be escorted during their visits.

Computer closets containing internet connections and switches require a key code for entry. Knowledge of the code is limited to three individuals. Smoke detectors and fire extinguishers are located throughout the building. For its cloud hosting service, CCR uses a third party subservice organization for its data center. Access to the data center is strictly controlled - the building itself is a non-descript building, with no indication that it houses electronic and computer equipment.

Access to the third party data center is controlled by key cards. CCR has been assigned four keycards. One is held by the Lead Tool Engineer. The other three are assigned to the VP of Professional Services and are used as floaters. The cards are kept in a locked drawer, and must be recorded in a log (maintained by a designated management member) when used. When the designated management member is scheduled to be out of the office, log book custody is given to the President/CEO.

The data center key cards are programmed to allow entrance to the data center building only through specific doors. Once in the building, card holders are restricted to certain areas of the building where CCR's equipment is located. Equipment is located in racks, which are secured through combination locks. CCR does not make the location of its racks within the data center generally available to employees - only employees who have a need to access the equipment know where CCR's racks are located. Data center employees do not have general access to CCR's systems.

Visitors must enter through the office door, and log into the sign-in sheet. They must be escorted by an authorized individual with a key card. Both must sign the sheet. The data center is responsible for providing the first line of physical security, meeting CCR's requirements, supported by a written contract. CCR monitors adherence with security and operational standards by direct observation. CCR also reviews the data center's service organization control report (SOC) for user control considerations and for resolution of reported exceptions.

E. System Components (Continued)

Control Activities (continued)

Physical Security Procedures (continued)

Access to offline storage, backup data, systems, and media is limited to computer operations staff through the use of physical and logical access controls. Backup data is stored on a server at the data center. Knowledge of server passwords is restricted to individuals designated by the Director of Professional Services.

Logical Security Procedures

Logical access to nonpublic information resources is protected through the use of native operating system security, native application, resource security, and add-on security software. User access is limited to the applications for which users are authorized and approved. Network and application authorization policies address password parameters around frequency, complexity, account lockout, length and history. Unique user IDs are assigned to individual users. System access for a user is disabled upon employee termination.

Redundant, high-availability firewalls are in place at the network perimeter to filter unauthorized inbound traffic. The firewalls are configured to deny any type of network connection that is not explicitly authorized by a firewall ruleset. The firewalls are configured to log a user out after a predefined period of inactivity. Unauthorized attempts to connect to a firewall and other events are logged and reviewed daily by CCR staff. The firewall systems require administrators to authenticate using a dual-factor authentication provided by AuthAnvil. Login requires user ID, login password, and entry of a system-generated code provided via a smart phone application. This one-use code is generated by a security token and synchronized to the server. Administrative privileges on the firewall systems are limited to selected individuals, as authorized by the Director of Professional Services.

Firewall monitoring is continual and 24/7. Certain thresholds have been set by management, and whenever a threshold is exceeded, an alert is sent by email and a ticket is created on the ConnectWise system. Daily, assigned staff reviews the emails and tickets and researches to resolve each issue. These are priority tasks each day. Intrusion detection systems provide continuous monitoring of CCR's network and early identification of potential security breaches. Updates, patches, etc. may be communicated by the manufacturer or identified by LabTech. Prior to installing updates, a form is prepared which outlines the required actions. The form must be signed by the Director of Professional Services.

All servers and desktops are protected by antivirus and spyware software to limit the possibility of disruptions. Any detection of viruses or spyware will result in the generation of a ticket for research and resolution. All email traffic pass through a third party spam filter. Only then is the email sent to CCR's mail server. Unneeded network services (for example, telnet, ftp, and http) are deactivated on CCR's servers.

Remote access is provided through ConnectWise Control. ConnectWise Control uses an AES-256 encryption algorithm to secure all data travelling across the communication path. The transmission is also configured with SSL to provide an additional lawyer of security for encryption key exchange. Both customers and CCR employees can access ConnectWise Control through an online portal.

E. System Components (Continued)

Control Activities (continued)

System Operations

Network performance and system processing are monitored using system monitoring tools by staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics are continually reviewed. Issues are addressed at monthly meetings.

The Company's ConnectWise system provides a ticket generation process for communicating and resolving issues and breaches. New employees receive training on the use of this system, and client users are informed about the process for generating tickets. User entities also may call the help desk, which will generate the ticket if the user opts, rather than generate the ticket online themselves.

An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.

Back-ups are created at least daily. Server files at the data center are backed up daily and housed on a separate server. A second backup is replicated at a second data center located elsewhere. Servers located at the client site are backed up and housed on a separate server at the client location. Clients can opt to retain a second copy at the data center. Both data center and client servers are monitored by LabTech and failures are reported via a ticket generated by ConnectWise.

CCR monitors for a wide variety of events, including:

- Event logs on remote servers
- Equipment failures
- Offline or system not available
- Email down
- Antivirus updates
- Backup failures
- Preventive maintenance (e.g. updates and patches)

An identified event will generate a ticket and send an email notification to responsible personnel. Responsible personnel research each event and work to resolve each issue. Resolution is documented on the ticket system. The network is protected by two layers of the SonicWALL firewall. If one fails, due to a hardware, software, or power issue, a second firewall will still protect the network against intrusion.

CCR has a documented business continuity and disaster recovery plan, which is updated in response to significant business changes, environmental changes, technology changes, and any other factor deemed by management as having a significant impact on CCR's ability to recover from a disaster situation..

E. System Components (Continued)

Control Activities (continued)

System Operations (continued)

CCR limits access to all servers and remote equipment. Access authorities are granted to employee users based on their job responsibilities. Access authorities for clients (user entities) are granted only as instructed by authorized individuals at clients. The system authenticates each user by verifying the username and password. Administrator access to client networks requires dual-factor authentication. The dual-factor authentication, provided by AuthAnvil, requires a username, password, and a system-generated code. The code is sent to a mobile device by phone call or text message. Access is authorized by the Director of Professional Services as part of the new user process.

If there is a need to use a storage media device, CCR requires that an encrypted USB drive be used. This device must be CCR owned equipment. All portable storage media that contains data or software must be stored by CCR personnel in a physically secured location when not in use.

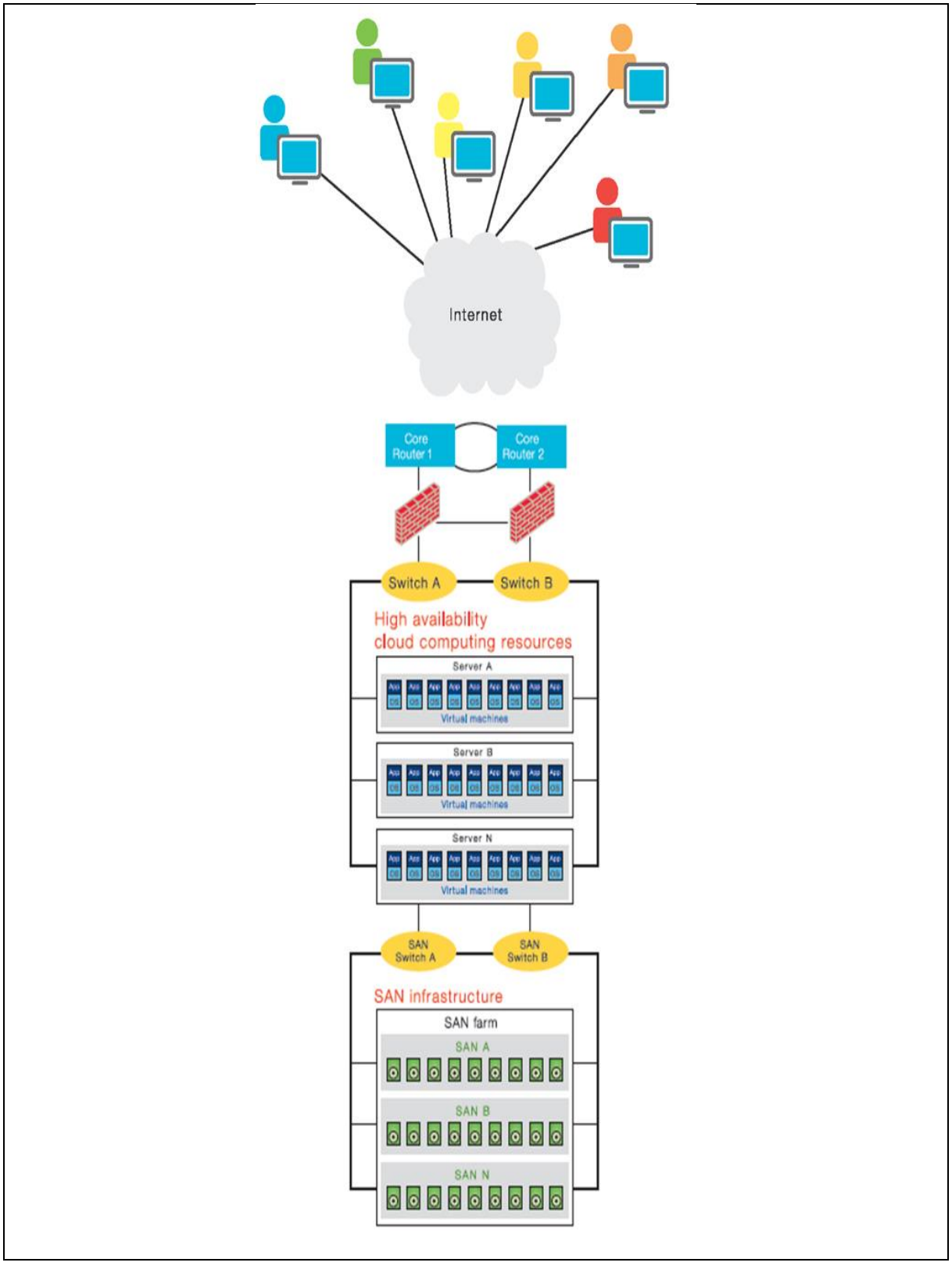
For hosted clients, a hypervisor firewall separates each client's data. No ports are open between clients, thus effectively keeping access restricted. All remote and mobile communication traffic is encrypted. The email communication sent to CCR mobile phones is encrypted when pulled from the email server. Encryption key management is fully automated (i.e., personnel do not have the opportunity to expose a key or influence the key creation). CCR uses the services of Entrust, who generates the encryption keys.

CCR has a defined equipment disposal process, designed to prevent customer data from being exposed to unauthorized individuals. When customers have equipment for disposal, a CCR tech will inspect the equipment and provide a quote. Once the quote is accepted, CCR will transport the equipment to a locked garage, until picked up by Advance Computer Recycling, a third party vendor. If requested by the customer, Advance Computer Recycling will provide a witnessed Certificate of Destruction, attesting that the equipment has been physically dismantled and hard drives destroyed (chipped) in accordance with industry standard practices. The entire process is controlled by a ConnectWise service ticket, which is not closed until all paperwork has been received back from the vendor.

E. System Components (Continued)

Control Activities (continued)

System Operations (continued)



SECTION IV

Trust Services Security Criteria and Controls Specified by Center for Computer Resources, LLC

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes user lists, transaction lists, and other populations we used for testing was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard "out of the box" reports as configured within the system
- Parameter-driven reports generated by systems or software
- Custom-developed scripts
- Spreadsheets that include relevant information utilized for the performance of testing of a control
- Prepared analyses, schedules, or other evidence

Our procedures to evaluate whether this information was sufficiently reliable, while not specifically called out in the test procedures listed in this section, were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by CCR.

Trust Services Criteria That Do Not Apply to the Service Organization

Criteria	Comments
CC1.2 – The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control	The service organization operates as a private company. Accordingly, it is not required by law or regulation to operate with an independent board of directors. Rather the service organization's top management are also its owners and directors. Accordingly, the manager/directors are involved in day to day operations, and may also be involved in delivering services to customers. Thus as a private company, this criteria does not apply.
CC1.3 – Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in pursuit of objectives.	As discussed in CC1.2, above, a board that is independent from management does not exist due to the service organization operating as a private entity that is not required to have such an independent body.

Trust Services Criteria and Related Controls

On the pages that follow, the description of the applicable trust services criteria and the controls to achieve the criteria have been specified by, and are the responsibility of CCR. .

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	CONTROL ENVIRONMENT		
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	1.1.1	The employee handbook includes sections covering security standards, workplace conduct, business ethics, and conflicts of interest that establish management's commitment to maintaining the highest levels of ethics and integrity.
		1.1.2	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies.
		1.1.3	New hires for key positions are required to complete background and drug screening prior to employment.
		1.1.4	Only those candidates holding industry specific certifications are considered for technical positions.
		1.1.5	New hires for technical roles are subject to approval by the Director of Professional Services prior to employment.
		1.1.6	Every employee has performance appraisals conducted by a Supervisor on an annual basis and related forms are maintained in the employee's personnel file.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.2.1	N/A - See section IV of system description
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.3.1	CCR management has an established organization chart to define and communicate organizational structures, authorities and reporting lines that impact the system. (See CC1.2 and section IV of system description)
		1.1.2 (Repeat Control)	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies. (See CC1.2 and section IV of system description)

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	CONTROL ENVIRONMENT		
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.1.2 (Repeat Control)	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies.
		1.1.3 (Repeat Control)	New hires for key positions are required to complete background and drug screening prior to employment.
		1.1.4 (Repeat Control)	Only those candidates holding industry specific certifications are considered for technical positions.
		1.1.5 (Repeat Control)	New hires for technical roles are subject to approval by the Director of Professional Services prior to employment.
		1.1.6 (Repeat Control)	Every employee has performance appraisals conducted by a Supervisor on an annual basis and related forms are maintained in the employee's personnel file.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.5.1	CCR has designated the Director of Professional Services as the Security Officer to ensure the maintenance and enforcement of the security policies.
		1.5.2	The Security Officer has custody of and is responsible for the day-to-day maintenance of the information security policies, and updates the policies as changes are needed, but at least annually.
		1.1.2 (Repeat Control)	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	COMMUNICATION AND INFORMATION		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1.1	CCR’s information systems capture data from a variety of monitoring tools (i.e. Automate/Auvik/SonicWALL GMS/etc.) regarding appropriate control activities that can be used in support of decision-making, and that alert support personnel.
		2.1.2	CCR's Service Desk/Assurance Team is responsible for logging information about system failures, incidents, and concerns. This information is logged in ConnectWise Manage as an incident ticket and reviewed by management to identify trends or unusual activity on a monthly basis.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	COMMUNICATION AND INFORMATION		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	2.2.1	Policies and procedures that document significant policies affecting security are available to employees on the corporate intranet.
		2.2.2	Employees sign an acknowledgment form within the employee handbook to acknowledge their understanding of the Company's policies, including security policies.
		2.2.3	New employees must sign an acceptable use agreement (AUA), signifying that they have read, understand, and will follow the security policies.
		2.2.4	Each year, employees must reconfirm their understanding of and compliance with the information security policies by signing the AUA.
		2.2.5	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.
		1.1.2 (Repeat Control)	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	COMMUNICATION AND INFORMATION		
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.3.1	Invoices and contracts describe the components and boundaries of the services provided.
		2.3.2	Security obligations of third party vendors are detailed in their contracts.
		2.3.3	Customer contracts contain information on how to communicate security incidents through the CCaRe Web portal or Help Desk Support.
		2.3.4	New customers are provided with instructions for communicating operational issues as part of CCR's onboarding process.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	RISK ASSESSMENT		
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1.1	CCR's risk management policy and risk management guidelines provide the Assurance Team with guidance to evaluate risk, quantitatively rate risk, and recommend changes to system or procedures. Recommendations for updates are reviewed by the CTO and approved by the executive management team.
		3.1.2	Each Team has KPI's that are reviewed weekly and evaluated for performance against both financial and operational goals.
		3.1.3	Current and potential risks to the system, management's risk tolerance, and the risk environment are reviewed weekly at Level 10 meetings.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	3.2.1	Management and department leaders meet annually to perform a documented review of their consideration of risk elements such as infrastructure, software, personnel and skills, threats and system security. The annual risk review includes consideration of Internal/external risks, management involvement, risk consideration/mitigation/acceptance, fraud risk, identification of assets and their related criticality, threats, and vulnerabilities.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.2.1 (Repeat Control)	Management and department leaders meet annually to perform a documented review of their consideration of risk elements such as infrastructure, software, personnel and skills, threats and system security. The annual risk review includes consideration of Internal/external risks, management involvement, risk consideration/mitigation/acceptance, fraud risk, identification of assets and their related criticality, threats, and vulnerabilities.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	RISK ASSESSMENT		
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	3.4.1	CCR has a policy that requires a formal vendor due diligence review of new significant vendors who may impact the system.
		3.4.2	CCR's Assurance team evaluates the effectiveness of controls by reviewing Root Cause Analysis (RCA) documents and ensure that mitigation strategies identified in these documents have been appropriately implemented. Additionally, the team reviews problem and major incident tickets to ensure that mitigations are in place for identified risks and recommends changes based on its evaluation. (i.e. FSRM to mitigate ransomware). The Assurance team also evaluates new technology and solutions against our current solutions for customers and CCR's needs and requirements.
		3.2.1 (Repeat Control)	Management and department leaders meet annually to perform a documented review of their consideration of risk elements such as infrastructure, software, personnel and skills, threats and system security. The annual risk review includes consideration of Internal/external risks, management involvement, risk consideration/mitigation/acceptance, fraud risk, identification of assets and their related criticality, threats, and vulnerabilities.
		2.2.5 (Repeat Control)	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.

TSC Ref. #	Criteria **MONITORING ACTIVITIES**	*Ctrl No.*	*CCR's Description of Controls.*
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	4.1.1	Network performance and system processing are monitored, using system monitoring tools, by IT staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics are recorded and compared to baseline statistics, and this information is considered in assessing the scope and frequency of monitoring activities.
		4.1.2	The information security team monitors the system and assesses the system vulnerabilities using proprietary and publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed, and implementations are monitored.
		4.1.3	Weekly Executive meetings are held to address system security concerns and trends.
		4.1.4	System performance, availability, capacity, and security concerns and trends are addressed at quarterly operations meetings.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	4.1.1 (Repeat Control)	Network performance and system processing are monitored, using system monitoring tools, by IT staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics are recorded and compared to baseline statistics, and this information is considered in assessing the scope and frequency of monitoring activities.
		4.1.2 (Repeat Control)	The information security team monitors the system and assesses the system vulnerabilities using proprietary and publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed, and implementations are monitored.
		4.1.3 (Repeat Control)	Weekly Executive meetings are held to address system security concerns and trends.
		4.1.4 (Repeat Control)	System performance, availability, capacity, and security concerns and trends are addressed at quarterly operations meetings.

TSC Ref. #	Criteria **CONTROL ACTIVITIES**	*Ctrl No.*	*CCR's Description of Controls.*
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	5.1.1	The Company has implemented a mix of preventative, detective, automatic and manual controls to manage risk to achieve objectives.
		1.5.1 (Repeat Control)	CCR has designated the Director of Professional Services as the Security Officer to ensure the maintenance and enforcement of the security policies and has custody of and is responsible for the day to day maintenance of the information security policies, and updates the policies as changes are needed, but at least annually.
		2.2.5 (Repeat Control)	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.
		4.1.3 (Repeat Control)	Weekly Executive meetings are held to address system security concerns and trends.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.2.1	IT general controls include a mix of preventative, detective, automatic and manual controls to manage risk to achieve objectives.
		2.2.5 (Repeat Control)	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.
		4.1.3 (Repeat Control)	Weekly Executive meetings are held to address system security concerns and trends.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	1.5.1 (Repeat Control)	CCR has designated the Director of Professional Services as the Security Officer to ensure the maintenance and enforcement of the security policies and has custody of and is responsible for the day to day maintenance of the information security policies, and updates the policies as changes are needed, but at least annually.
		2.2.1 (Repeat Control)	Policies and procedures that document significant policies affecting security are available to employees on the corporate intranet.
		4.1.3 (Repeat Control)	Weekly Executive meetings are held to address system security concerns and trends.

TSC Ref. #	Criteria	Ctrl No.	CCR's Description of Controls.
	LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	6.1.1	Access rules and groups have been defined for all confidential access.
		6.1.2	Users must establish their identity to the entity's network and application systems when accessing resources through the use of a valid user ID that is authenticated by an associated password.
		6.1.3	Passwords are case sensitive and must contain a required minimum number of characters, with the use of at least three of the four character types. The network is also configured to enforce password expiration internals, invalid password lockout, and password history rules.
		6.1.4	Administrative access requires the use of dual-factor authentication provided by AuthAnvil. Login requires a user ID, login password, and a one-use, system-generated code provided via a smart phone application for authentication.
		6.1.5	Internal users' access to IT Glue requires multi-factor authentication: user name, password, and a one-time use code generated by Google Authenticator via a smart phone app.

TSC Ref. #	Criteria	Ctrl No.	CCR's Description of Controls.
	LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	6.2.1	Unique user IDs are assigned to individual users as part of the new user process.
		6.2.2	The ability to create or modify users and change user access privileges in ConnectWise is limited to authorized personnel.
		6.2.3	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.
		6.2.4	Management performs a periodic review of access authorities for accuracy. An Access Rights Review Form is used to document the review. A member of senior management without administrative rights is required to review the form and access authorities report, and document his review by signing the form.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	6.3.1	Access to confidential information and restricted resources is based on job need. Access is authorized by the Director of Professional Services as part of the new user process.
		6.2.2 (Repeat Control)	The ability to create or modify users and change user access privileges in ConnectWise is limited to authorized personnel.
		6.2.3 (Repeat Control)	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.
		6.2.4 (Repeat Control)	Management performs a periodic review of access authorities for accuracy. An Access Rights Review Form is used to document the review. A member of senior management without administrative rights is required to review the form and access authorities report, and document his review by signing the form.

TSC Ref. #	Criteria **LOGICAL AND PHYSICAL ACCESS CONTROLS**	*Ctrl No.*	*CCR's Description of Controls.*
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.4.1	Access to the third-party data center is controlled by electronic key cards, whose access is limited to designated individuals within the Company.
		6.4.2	Exterior entrances to the facility are locked and access is restricted via badge/keycard access.
		6.2.3 (Repeat Control)	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.4.1 (Repeat Control)	Access to the third-party data center is controlled by electronic key cards, whose access is limited to designated individuals within the Company, and logged.
		6.2.3 (Repeat Control)	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.6.1	Email communication is secured through the use of appropriate third party email services, including filtering of email spam and scanning of files for viruses, spyware, and malware.
		6.6.2	Redundant firewalls are used and configured to prevent unauthorized access. Hypervisor firewall events are logged and reviewed daily by the Security Officer. SonicWall firewall is integrated to ConnectWise and events automatically generate a ticket for research and resolution.
		6.6.3	Intrusion detection systems are used to provide continuous monitoring of the system and early identification of potential security breaches.

TSC Ref. #	Criteria	Ctrl No.	CCR's Description of Controls.
	LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	6.7.1	The entity uses industry standard encryption technology for the transmission of private or confidential information over public networks, including user IDs and passwords.
		6.7.2	Entity policies prohibit the transmission of confidential or sensitive information over the Internet or other public communications paths unless it is encrypted.
		2.2.4 (Repeat Control)	Each year, employees must reconfirm their understanding of and compliance with the information security policies by signing the AUA.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	6.8.1	Antivirus and antispyware programs are in place on all computers and servers, including scans of incoming email messages.
		6.8.2	The Labtech management system monitors servers and computers for a wide variety of events, including infections and updates to antivirus and antispyware programs.
		6.8.3	Security events (such as virus detection or antivirus updates) generate a ticket for research and resolution.
		6.8.4	Email traffic is first routed to an offsite spam filter, and then routed to the CCR email server.
		6.8.5	The ability to install, modify, and replace operating system and other system programs is restricted to authorized personnel, as designated by the Director of Professional Services.
		6.8.6	Access to superuser functionality and sensitive system functions is restricted to authorized personnel, as designated by the Director of Professional Services.

TSC Ref. #	Criteria SYSTEM OPERATIONS	*Ctrl No.*	*CCR's Description of Controls.*
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	7.1.1	CCR maintains risk appropriate baseline configuration standards to ensure that devices meet organizational needs. Baselines are reviewed and/or updated at least annually. Tools used include Auvik and SonicWALL GMS.
		7.1.2	CCR monitors compliance with baseline configuration standards for infrastructure devices, servers and end-user stations using automated tools. Deviation from standards are handled as incidents and an incident ticket is generated in ConnectWise Automate. The incident is investigated and remediated, or scanning tools are updated. CCR employs multiple detection systems inside of system boundaries to identify unauthorized resources. Events are logged in ConnectWise Manage.
		7.1.3	CCR conducts at least weekly vulnerability scans of internal assets and customer hosted systems to identify potential vulnerabilities. CCR uses vulnerability priority ratings to prioritize remediation of vulnerabilities identified. Tickets in ConnectWise Automate are generated and configuration updates are implemented using the standard change management process.
		7.1.4	CCR maintains a complete inventory of the system's hardware and software components that is updated daily for changes. New and unknown assets are investigated by the Assurance Team to ensure that assets are authorized.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	4.1.1 (Repeat Control)	Network performance and system processing are monitored, using system monitoring tools, by IT staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics are recorded and compared to baseline statistics, and this information is considered in assessing the scope and frequency of monitoring activities.
		4.1.2 (Repeat Control)	The information security team monitors the system and assesses the system vulnerabilities using proprietary and publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed, and implementations are monitored.
		4.1.4 (Repeat Control)	System performance, availability, capacity, and security concerns and trends are addressed at quarterly operations meetings.
		6.6.4 (Repeat Control)	Intrusion detection systems are used to provide continuous monitoring of the system and early identification of potential security breaches.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	SYSTEM OPERATIONS		
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	7.3.1	Intrusion detection systems and other tools are used to identify, log, and report potential security breaches and other incidents. Monitoring systems are integrated to ConnectWise. The system notifies the responsible network administrator via e-mail and a ticket is generated for potential incidents in progress. When a significant incident is detected or reported, a defined incident management process is initiated and the Director of Professional Services is notified. The Director will lead the effort to perform the rest of the process. Corrective actions are implemented in accordance with the incident response plan.
		7.3.2	The ConnectWise system provides dashboards for management monitoring of open tickets. Individuals assigned to resolving tickets document the final resolution on the ticket.
		4.1.3 (Repeat Control)	Weekly Executive meetings are held to address system security concerns and trends.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	7.3.1 (Repeat Control)	Intrusion detection systems and other tools are used to identify, log, and report potential security breaches and other incidents. Monitoring systems are integrated to ConnectWise. The system notifies the responsible network administrator via e-mail and a ticket is generated for potential incidents in progress. When a significant incident is detected or reported, a defined incident management process is initiated and the Director of Professional Services is notified. The Director will lead the effort to perform the rest of the process. Corrective actions are implemented in accordance with the incident response plan.
		7.3.2 (Repeat Control)	The ConnectWise system provides dashboards for management monitoring of open tickets. Individuals assigned to resolving tickets document the final resolution on the ticket.
		2.2.1 (Repeat Control)	Policies and procedures that document significant policies affecting security are available to employees on the corporate intranet.
		2.2.5 (Repeat Control	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	SYSTEM OPERATIONS		
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.3.1 (Repeat Control)	Intrusion detection systems and other tools are used to identify, log, and report potential security breaches and other incidents. Monitoring systems are integrated to ConnectWise. The system notifies the responsible network administrator via e-mail and a ticket is generated for potential incidents in progress. When a significant incident is detected or reported, a defined incident management process is initiated and the Director of Professional Services is notified. The Director will lead the effort to perform the rest of the process. Corrective actions are implemented in accordance with the incident response plan.
		7.3.2 (Repeat Control)	The ConnectWise system provides dashboards for management monitoring of open tickets. Individuals assigned to resolving tickets document the final resolution on the ticket.
		2.2.5 (Repeat Control	An incident response plan exists for the identification and escalation of security breaches and other incidents. It includes information concerning the identification of possible security breaches and the process of informing the security team.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	CHANGE MANAGEMENT		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	8.1.1	All change requests require completion of a Change Management Request form. The form includes the type of request, the impact, resources needed, a risk assessment, an implementation plan, and a rollback plan if complications ensue. The form requires approval of the Director of Professional Services or President.
		8.1.2	All employees are required to sign an Acceptable Use Agreement (both initially and annually), which clearly spells out that only authorized system changes are allowed.
		8.1.3	Emergency changes are standardized and subject to ConnectWise ticket generation and/or Change Management Request Form depending on the type of change. Open tickets will appear on dashboards for management monitoring. Client change requestors are kept informed about the status of their requests verbally or by email.
		8.1.4	Documented change management procedures are in place to guide personnel in performing application, system, hardware, software and network related changes. Procedures include roles, responsibilities, and actions required to implement emergency changes.
		8.1.5	All change requests from clients are entered into the ConnectWise system, which generates a ticket. The ticket must be initiated by an authorized client user and all tickets are subject to documentation requirements and management review. The client predetermines which individuals are authorized to make such requests, and those individuals are listed in the client profile section of ConnectWise.

TSC Ref. #	Criteria	*Ctrl No.*	*CCR's Description of Controls.*
	RISK MITIGATION		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	9.1.1	CCR maintains professional liability and business continuity insurance policies that are evaluated annually. The policy is reviewed by the Executive management team prior to policy renewals.
		3.4.1 (Repeat Control)	CCR conducts formal risk assessments on third-parties and vendors as part of the risk assessment process, using surveys to evaluate the security posture and risk introduced.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	9.2.1	The Company obtains a SOC report for its subservice data center to engable identification of risks, and may also conduct site visits as deemed necessary.
		3.4.1 (Repeat Control)	CCR has a policy that requires a formal vendor due diligence review of new significant vendors who may impact the system.