Center for Computer Resources, LLC.

Description of the Managed IT Services System

SOC 2 Type 2 Report

For the Period September 1, 2016, to August 31, 2017

Cohen & Co

cohencpa.com

CENTER FOR COMPUTER RESOURCES, LLC.

FOR THE PERIOD SEPTEMBER 1, 2016, TO AUGUST 31, 2017

TABLE OF CONTENTS

SECTION I

Independent Service Auditors' Report

Cohen & Co

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy

Scope

We have examined the description in Section 3 titled "Center for Computer Resources, LLC. *Description of the Managed IT Services System for the Period September 1, 2016 to August 31, 2017*" (description) based on the criteria set forth in Paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security principle set forth in *TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016) (applicable trust services criteria), throughout the period September 1, 2016, to August 31, 2017. The controls included in the description are those that management of CCR believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Managed IT Services System that are not likely to be relevant to meeting the applicable trust services criteria. The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of CCR's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the description, CCR uses service organizations (subservice organization) to perform cloud hosting services. The description indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of CCR's controls are suitably designed and operating effectively, along with the related controls at CCR. The description presents CCR's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

In Section 1, Center for Computer Resources has provided its assertion titled "Assertion of the Management of Center for Computer Resources, LLC. Regarding its Managed IT Services System" (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Center for Computer Resources, LLC. is 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; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls that are suitably designed and operating effectively to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period September 1, 2016, to August 31, 2017. 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 and operating effectiveness of controls involves -

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period September 1, 2016 to August 31, 2017.
- assessing the risks that the description is not fairly presented based on the description criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the applicable trust services criteria stated therein, and the suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important in its own particular environment. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria identified in CCR's assertion and the applicable trust services criteria -

a) the description fairly presents the system that was designed and implemented throughout the period September 1, 2016, to August 31, 2017.

b) the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period September 1, 2016, to August 31, 2017, and the subservice organization applied the complementary controls assumed in the design of Center for Computer Resources Inc.'s controls throughout the period September 1, 2016, to August 31, 2017, and user entities applied the complementary user entity controls assumed in the design of Center for Computer Resources' controls throughout the period September 1, 2016, to August 31, 2017.

c) the controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period September 1, 2016, to August 31, 2017, if the complementary subservice organization controls assumed in the design of Center of Computer Resources' controls operated effectively throughout the period September 1, 2016, to August 31, 2017, if user entities applied the complementary user entity controls assumed in the design of Center for Computers Resources' controls, and those controls operated effectively throughout the period September 1, 2016, to August 31, 2017.

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are listed in Section V, *"Trust Services Security Principle, Criteria, Related Controls, and Tests of Controls"* of this report.

Restricted Use

This report, including the description of tests of controls and results thereof in Section V, is intended solely for the information and use of Center for Computer Resources, LLC.; user entities of Center for Computer Resources' Managed IT Services System during some or all of the period September 1, 2016, to August 31, 2017; and prospective user entities, independent auditors, and practitioners providing services to such user entities, 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, subservice organizations, and other parties.
- Internal control and its limitations.
- The nature of user entity controls and responsibilities, and their role in the user entity's internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

Cohen & Company Ltd.

January 18, 2018
St. Clair Shores, Michigan

SECTION II

Assertion of the Management of Center for Computer Resources, LLC. Regarding the Managed IT Services System

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. Regarding the Managed IT Services System

We have prepared the description titled Managed IT Services System (description) based on the criteria for a description of a service organization's system identified in *Paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Managed IT Services System, particularly system controls intended to meet the criteria for the security principle set forth in *TSP 100 (2016), Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period September 1, 2016, to August 31, 2017.

Center of Computer Resource, LLC (the Company) uses a subservice organization for data center / cloud hosting services. The description includes only the applicable trust services criteria and related controls of Center for Computer Resources, Inc. and excludes the applicable trust services criteria and related controls of the subservice organization. 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 the applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Center for Computers Resources' controls are suitably designed and operating effectively, along with related controls at the service organization and the subservice organization. The description does not extend to controls of the user entities.

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

1. The description fairly presents the Managed IT Service System throughout the period September 1, 2016, to August 31, 2017 as it relates to controls that are likely to be relevant to meeting the applicable trust services criteria. Our assertion is based on the following description criteria:

    a) The description contains the following information:

        i) The types of services provided.

        ii) The components of the system used to provide the services, which are as follows:

        iii)

            (1) *Infrastructure.* The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

            (2) *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

            (3) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

            (4) *Processes.* The automated and manual procedures.

            (5) *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

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

iv) The boundaries or aspects of the system covered by the description.

v) For information provided to, or received from, subservice organizations, and other parties -

(1) how the information is provided or received and the role of the subservice organizations and other parties.

(2) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

vi) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization's system.

(2) When the inclusive method is used to present a subservice organization, controls at the subservice organization.

vii) If the service organization presents the subservice organization using the carve-out method:

(1) the nature of the services provided by the subservice organization.

(2) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

viii) Any applicable trust services criteria that are not addressed by a control and the reasons.

ix) In the case of a Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

b) The description does not omit or distort information relevant to the service organization's system while acknowledging that 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 each individual report user may consider important to its own particular needs.

2) The controls stated in the description were suitably designed throughout the period September 1, 2016, to August 31, 2017 to meet the applicable trust services criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of Center for Computers Resources, LLC's controls throughout the period September 1, 2016, to August 31, 2017.

3) The controls stated in the description operated effectively throughout the period September 1, 2016, to August 31, 2017 to meet the applicable trust services criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of Center for Computer Resources, LLC's controls throughout the period September 1, 2016, to August 31, 2017.

Joe D Barby Partner

Signature & Title

January 18, 2018

SECTION III

Center for Computer Resources, LLC. Description of the Managed IT Services System for the period September 1, 2016, to August 31, 2017

Company 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

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 and 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.

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

CCaRe 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.

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 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. It 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 and 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.

Use of Subservice Organization

The Company uses a subservice organization for data center / cloud hosting services. The control objectives impacted by the subservice organization and related control activities are not 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. Management expects that the subservice organization will have certain types of controls in place, which include:

- Controls supporting an adequate control environment
- Risk assessment, information and communication and monitoring activity controls
- Information technology general controls covering physical, logical and environmental security
- Disaster recovery plans
- Data backup and recovery controls
- Change management controls
- Role based or similar access controls

The following components related to the security trust services criteria applicable to the system can only be met if controls at the subservice organization are suitably designed and implemented to address the following specified security criteria:

CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security are communicated to those users in a timely manner.
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments, and system requirements as they relate to security.
CC5.6	Logical access security measures have been implemented to protect against security threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security.
CC6.1	Vulnerabilities of system components to security breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security.
CC6.2	Security incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.

CC7.1	The entity's commitments and system requirements, as they relate to security, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security.

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.

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

Control activities related to the Company's applicable Trust Services Principles 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 and user activities and the consequences of non-compliance. An AUA is a key activity for user awareness and administrative policing of system activities.

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 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.

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. They 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 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.

System Components

Infrastructure

CCR uses a third party subservice organization for data center / 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, redundant4 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

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 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. In December 2016, CCR started to implement 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.

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.

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 their 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 Leads 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.

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 and 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 the entity'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 the entity'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 the online portal.

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. Clients also may call the help desk, who will generate the ticket if clients opt, 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.

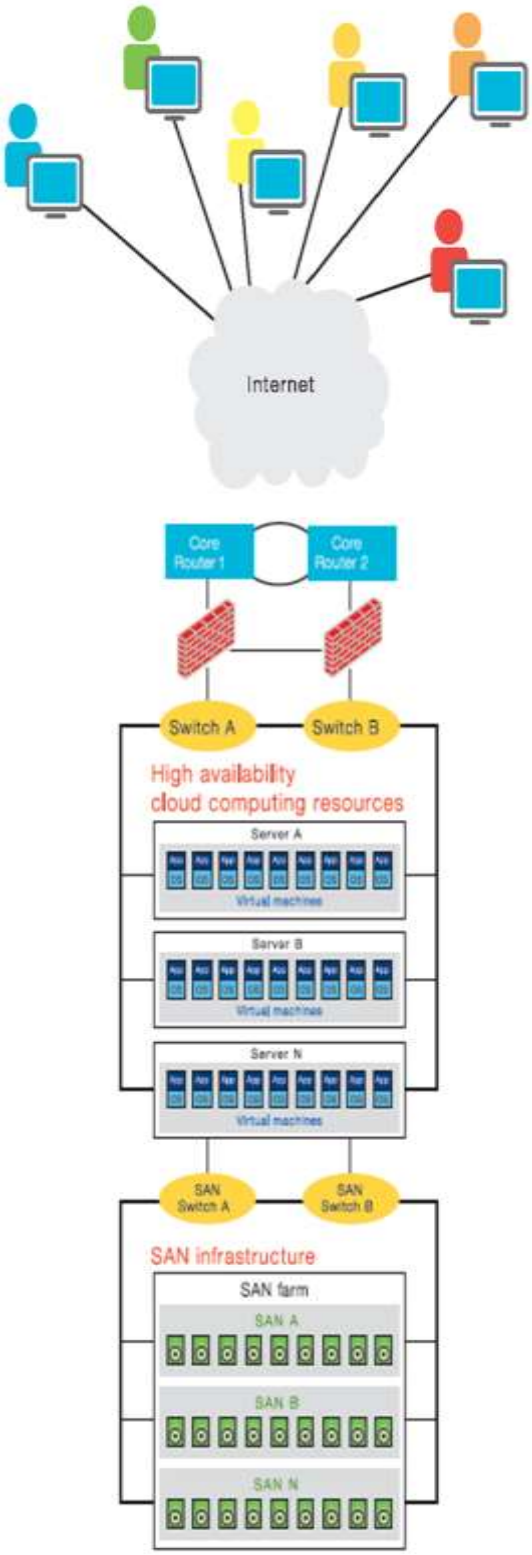
CCR has a documented business continuity and disaster recovery plan, which is updated as necessary.

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 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.


Internet
Core Router 1
Core Router 2
Switch A
Switch B
High availability cloud computing resources
Server A
Server B
Server N
Virtual machines
SAN Switch A
SAN Switch B
SAN infrastructure
SAN farm
SAN A
SAN B
SAN N

DATA CENTER ARCHITECTURE OVERVIEW

FACILITIES

- Redundant fiber connections to multiple Internet providers
- Hospital-grade diesel generator with priority re-fueling contracts with multiple fuel vendors
- Three Liebert online uninterruptable power supply battery backup units
- Redundant Liebert air conditioning units
- Pre-action fire suppression system
- Facilities are monitored 24x7x365
- Secure access controls to data center

SERVERS AND INFRASTRUCTURE

- Redundant and load balanced server farm optimized for virtualization
- Redundant and load balanced SANs with redundant fabric and SAN replication
- Redundant network paths throughout

SECURITY

- High availability enterprise class firewalls
- Gateway anti-virus, antispyware, and content filtering
- Intrusion Prevention System and Intrusion Detection System
- Hypervisor-based firewall securing and isolating each individual virtual machine
- Automated audit trails for all systems including hardware, virtualization and Windows layers
- Protection of all WAN traffic using a combination of SSL and IPSEC encryption

FULLY MANAGED

- Nightly back-up and disaster recovery services
- Proactive monitoring of all systems
- Updated antivirus/ antispyware/ antispam and patches
- Hardware upgrades and maintenance
- Always available help desk support

SECTION IV

Complementary User Entity Controls

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 principles 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.

The following trust services criteria can be achieved only if relevant complementary user entity controls contemplated in the design of Center for Computer Resources' controls are suitably designed, along with related controls at CCR:

Criteria Category	Criteria
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security.

CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security.
CC5.6	Logical access security measures have been implemented to protect against security threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security.
CC6.2	Security incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.

Control Considerations for the User Entity:

1. The user entity is responsible for understanding and complying with their contractual obligations to Center for Computer Resources.

2. The user entity is responsible for ensuring that data input or retrieved from its systems are in accordance with user entity policy, and are limited to authorized personnel.

3. 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.

4. The user entity is responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with the system.

5. The user entity is responsible for user accounts that need to be added or removed due to employee termination or transfer of job responsibilities.

6. The user entity is responsible for securing the method to request and remove access to ensure that appropriate users are requesting access to systems.

7. The user entity is responsible for monitoring access to its systems, and to insure that only authorized users are accessing them and that any unauthorized access or security incidents are reported to CCR.

8. The user entity is responsible for ensuring the communications method utilized to connect to hosted servers are secure from internal and external threats.

9. The user entity is responsible for developing their own disaster recovery and business continuity plans to supplement the CCR services.

SECTION V

Trust Services Security Principles, Criteria, Related Controls, and Tests of Controls

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC1.0	**Common Criteria Related to Organization and Management**				
CC 1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security.	1.1.1	CCR management has an established organization chart to define and communicate organizational structures, authorities and reporting lines that impact the system.	Inquired of the CEO to verify that an organization chart is maintained and communicated to CCR personnel.	**No exceptions noted**
				Inspected the organizational chart to verify that roles, and responsibilities were defined in the form of cascading reporting lines of authority.	**No exceptions noted**
		1.1.2	Roles and responsibilities are defined in written job descriptions. Roles and responsibilities are also documented in the information technology policies.	Inspected a sample of job descriptions to ensure documentation of roles and responsibilities.	**No exceptions noted**
CC 1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security.	1.2.1	CCR has designated the Director of Professional Services as the Security Officer to ensure the maintenance and enforcement of the security policies.	Inquired of the CEO to verify the Director of Professional Services has been designated as the Security Officer, responsible for the maintenance and enforcement of the security policies.	**No exceptions noted**
		1.2.2	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.	Inspected the information security policies and employee handbook, noting the Security Officer's annual review of policies.	**No exceptions noted**
		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.	Inspected the security policies to ascertain whether they include section headings that address the area of responsibility and accountability of the policy to the Security Officer.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and provides resources necessary for personnel to fulfill their responsibilities.	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.	Inspected written job descriptions noting job responsibilities are included and are available on the intranet.	**No exceptions noted**
		1.3.1	New hires for key positions are required to complete background and drug screening prior to employment	Inspected the personnel records for a sample of new employees hired during the period for evidence of completed background and drug screenings.	**No exceptions noted**
		1.3.2	Only those candidates holding industry specific certifications are considered for technical positions.	Inspected the personnel file for new employees hired during the period noting evidence that they possessed the requisite technical skills.	**No exceptions noted**
		1.3.3	New hires for technical roles are subject to approval by the Director of Professional Services prior to employment.	Inspected personnel files for new employees hired during the period, noting the approval of the Director of Professional Services.	**No exceptions noted**
		1.3.4	Every employee has performance appraisals conducted by a Supervisor on an annual basis and related forms are maintained in the employee's personnel file.	Inquire of the CEO whether performance appraisals are performed on an annual basis.	**No exceptions noted**
				Inspected a sample of personnel files for evidence that an annual performance appraisal was performed.	**Exceptions noted.** Out of a sample of 34 personnel files examined, we identified 3 employee files that were not evaluated by the Supervisor.

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security.	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.	Inspected written job descriptions noting job responsibilities are included and are available on the intranet.	**No exceptions noted**
		1.4.1	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.	Inspected the employee handbook, to verify that the handbook covered security standards, workplace conduct, business ethics, and conflicts of interest.	**No exceptions noted**
		1.3.1 (Repeat Control)	New hires for key positions are required to complete background and drug screening prior to employment	Inspected the personnel records for a sample of new employees hired during the period for evidence of completed background and drug screenings.	**No exceptions noted**
		1.3.2 (Repeat Control)	Only those candidates holding industry specific certifications are considered for technical positions.	Inspected the personnel file for new employees hired during the period noting evidence that they possessed the requisite technical skills.	**No exceptions noted**
		1.3.3 (Repeat Control)	New hires for technical roles are subject to approval by the Director of Professional Services prior to employment..	Inspected personnel files for new employees hired during the period, noting the approval of the Director of Professional Services.	**No exceptions noted**
		1.3.4 (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.	Inquired of the CEO whether performance appraisals are performed on an annual basis.	**No exceptions noted**
				Inspected a sample of personnel files for evidence that an annual performance appraisal was performed.	**Exceptions noted. Out of a sample of 34 personnel files examined, we identified 3 employee files that were not evaluated by the Supervisor.**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC2.0	**Common Criteria Related to Communications**				
CC 2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	2.1.1	Policies and procedures that document significant policies affecting security are available to employees on the corporate intranet.	Inspected the employee handbook and information security policies to verify documentation of standards related to security, noting the handbook and policies were available on the corporate intranet.	**No exceptions noted**
		2.1.2	Invoices and contracts describe the components and boundaries of the services provided.	Inspected a sample of invoices, noting detailed description of services, including components and boundaries of the services.	**No exceptions noted**
				Inspected a sample of customer contracts, noting description of services, including components and boundaries of the services.	**No exceptions noted**
		1.1.1 (Repeat Control)	CCR management has an established organization chart to define and communicate organizational structures, authorities and reporting lines that impact the system.	Inquired of the CEO to verify that an organization chart is maintained and communicated to CCR personnel.	**No exceptions noted**
				Inspected the organizational chart to verify that roles, and responsibilities were defined in the form of cascading reporting lines of authority.	

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 2.2	The entity's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	2.2.1	Employees sign an acknowledgment form within the employee handbook to acknowledge their understanding of the Company's policies, including security policies.	Inspected a sample of employees personnel files noting there was a signed acknowledgement form retained in the employee personnel file.	**No exceptions noted**
		2.2.2	New employees must sign an acceptable use agreement (AUA), signifying that they have read, understand, and will follow the security policies.	Inspected all new employees' personnel files noting there was a signed acceptable use agreement retained.	**No exceptions noted**
		2.2.3	Each year, employees must reconfirm their understanding of and compliance with the information security policies by signing the AUA.	Inspected a sample of employee personnel files noting they signed the employee handbook which includes the security policies.	**No exceptions noted**
		2.2.4	Security obligations of third party vendors are detailed in their contracts.	Inspected the signed contractor agreement which indicates the security obligations of contractors.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	1.2.2 (Repeat Control)	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.	Inspected the information security Policies and employee handbook, noting the Security Officer's annual review of policies.	**No exceptions noted**
		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.	Inspected written job descriptions noting job responsibilities are included and are available on the intranet.	**No exceptions noted**
		2.1.2 (Repeat Control)	Invoices and contracts describe the components and boundaries of the services provided.	Inspected a sample of invoices, noting detailed description of services, including components and boundaries of the services.	**No exceptions noted**
				Inspected a sample of customer contracts, noting description of services, including components and boundaries of the services.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system is provided to personnel to carry out their responsibilities	2.1.1 (Repeat Control)	Policies and procedures that document significant policies affecting security are available to employees on the corporate intranet.	For a sample of new hires, inspect training documents to confirm that new hires received security awareness training.	**No exceptions noted**
		2.1.2 (Repeat Control)	Invoices and contracts describe the components and boundaries of the services provided.	Inspected a sample of invoices, noting detailed description of services, including components and boundaries of the services.	**No exceptions noted**
				Inspected a sample of customer contracts, noting description of services, including components and boundaries of the services.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 2.5	Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	2.5.1	Customer contracts contain information on how to communicate security incidents through the CCaRe Web portal or Help Desk Support.	Inquired of the CEO, CFO and corroborated with the Security Officer, customer contracts contain information on how to communicate security incidents through the CCaRe Web portal or Help Desk Support.	**No exceptions noted**
				Inspected the ConnectWise incident tracking systems and noted that customers have capability to generate tickets.	**No exceptions noted**
		2.5.2	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.	Inspected the Company's incident response plan, noting that the plan identifies possible security breaches and the process for informing the security team.	**No exceptions noted**
		2.5.3	New customers are provided with instructions for communicating operational issues as part of CCR's onboarding process.	Inspected the onboarding template noting that instructions for communicating operational issues were included in the document.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC 2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security are communicated to those users in a timely manner.	2.6.1	Planned changes to system components and the scheduling of those changes are reviewed as part of department meetings.	Inspected a sample of weekly meeting agendas, noting the section where system changes would appear.	**No exceptions noted**
		2.6.2	Changes to system components, including those that may affect system security, require the approval of the Security Officer or CEO before implementation.	Inquired of the VP of Sales that meetings address changes of system components including those that effect system security.	**No exceptions noted**
				Inspected the only change form during the period, noting the approval from the Security Officer.	**No exceptions noted**
		2.6.3	Changes that may affect system security are discussed with affected clients for review and approval prior to implementation.	Inquired of the Security Officer that changes that may affect system security are discussed with affected clients for review and approval prior to implementation.	**No exceptions noted**
				Inspected the incident response plan noting the communication sections, which details the communication policy that affect system security.	**No exceptions noted. We further noted that there were no such changes during the examination period.**
		2.6.4	There is periodic communication of changes, orally and/or by email, including changes that affect security.	Inspected all emails sent by the Security Officer during the period, noting that ongoing routine maintenance performed, that could impact security, was communicated to applicable users.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**				
CC 3.1	The entity: (1) identifies potential threats that could impair system security commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system) (2)analyzes the significance of risks associated with the identified threats, (3)determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	3.1.1	Management and department leaders periodically meet to review and evaluate risk elements such as infrastructure, software, people, threats and system security.	Inspected a sample of minutes from weekly executive meetings, noting a section regarding risk assessment, which described threats and the risks involved with these threats.	**No exceptions noted**
		2.5.2 (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.	Inspected the Company's incident response plan, noting the identification of possible security breaches and the process for informing the security team.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	3.2.1	CCR has established policies and procedures that affect system security requirements as part of its risk assessment program.	Inquired of the CFO and CEO as to whether CCR has established policies and procedures that affect system security requirements as part of its risk assessment program.	**No exceptions noted**
		3.2.2	CCR has documented and defined critical scurity elements such as logical and physical access, roles, and responsibilities in an information security policy.	Inspected the information security policies noting critical security elements relevant to the system are deliniated.	**No exceptions noted**
		2.5.2 (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.	Inspected the Company's incident response plan, noting that the plan identifies possible security breaches and the process for informing the security team.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC4.0	**Common Criteria Related to Monitoring of Controls**				
CC 4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	4.1.1	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.	Inquired of the Security Officer that monitoring systems are in place to monitor network performance and system availability.	**No exceptions noted**
				Inspected settings within the ConnectWise system noting the events that would generate an alert, and that a ticket is automatically generated in ConnectWise after the time parameters for a specific event have been met.	**No exceptions noted**
		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.	Inspected a sample of Weekly Executive Meetings noting that the results of monitoring activities are discussed and actions taken as management considered necessary.	**No exceptions noted**
		4.1.3	Weekly Executive meetings are held to address system security concerns and trends.	Inspected a sample of Weekly Executive Meetings noting that system security concerns and trends are discussed.	**No exceptions noted**
		4.1.4	System performance, availability, capacity, and security concerns and trends are addressed at quarterly operations meetings.	Inspected a copy of quarterly meeting minutes that occurred during the period, noting that management reviews system components such as CPU performance, utilization and security risk.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**				
CC 5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security.	5.1.1	Logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security, and add-on security software.	Inquired of the Security Officer and The Lead Tools Engineer that logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security and add on security software.	**No exceptions noted**
				Inspected the domain group policy noting that logon and complex passwords are required to gain access to the network.	**No exceptions noted**
				Observed a tools Engineer log into the Lab Tech security software noting that employees require a logon and password to gain access to the program.	**No exceptions noted**
		5.1.2	Access to confidential information and restricted resources is based on job need. Access is authorized by the Director of Professional Services or the Lead Tools Engineer as part of the new user process.	Inspected new employees hired within the examination period noting that access is authorized by the Director of Professional Services or the Lead Tools Engineer.	**No exceptions noted**
		5.1.3	Access rules and groups have been defined for all confidential access.	Inspected rules and rights list from the software program indicating the different access rules and groups have been defined when available.	**No exceptions noted**
		5.1.4	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.	Inspected a list of user ID's noting that each user has a unique user-ID which will grant them access to electronic resources.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
		5.1.5	Clients accessing the client ticketing portal can only view their data.	Observed an associate access a specified client's ticketing portal by using an appropriate user id and password, noting that only that client's data was available for viewing in the portal.	**No exceptions noted**
		5.1.6	Access to offline storage, backup data, systems, and media is limited to computer operations staff through the use of electronic keycards needed to access the third-party data center.	Inquired of the Security Officer, who has custody of keycards, noting the Security Officer and system administrator have keycards and spare floater cards are assigned to employees by the Security Officer and a log is retained.	**No exceptions noted**
				Inspected the keycard log noting the log included who used the card, when it was used and why.	**No exceptions noted**
		5.1.7	Hardware and operating system configuration tables are restricted to authorized personnel through physical access controls, native operating system security, and add-on security software.	Inspected the keycard log noting the log included who used the card, when it was used and why.	**No exceptions noted**
				Inquired of the Security Officer, a network administrator and an escalating engineer that only authorized users have knowledge of master user passwords of hardware and operating system configuration tables.	**No exceptions noted**
		5.1.8	Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff.	Inspected the utility program user listing, noting that the ability to add/change or delete users are restricted to authorized technical services staff.	**No exceptions noted**
		5.1.9	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.	Observed an administrative user attempt to gain access and be denied access with the dual factor software by supplying a user id, password, and a one-time system generated pin.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	5.1.2 (Repeat Control)	Access to confidential information and restricted resources is based on job need. Access is authorized by the Director of Professional Services or the Lead Tool Engineer as part of the new user process.	Inspected a list of newly hired employees noting that the Director of Professional Services authorized access.	**No exceptions noted**
		5.2.1	Requests to make changes to client users must be generated by the client via the ConnectWise ticket generation process, and must be approved by an authorized client employee.	Inspected a sample of tickets generated in ConnectWise by clients, noting that a request for new employee access was authorized by designated individuals.	**No exceptions noted**
				Observed a user access customer information using the ConnectWise system, noting a message occurs indicating those who are authorized to add/change/delete users.	**No exceptions noted**
		5.2.2	The ability to create or modify users and change user access privileges in ConnectWise is limited to authorized personnel.	Inspected the ConnectWise software program noting the ability to create or modify users was limited to the Director of Professional Services and a Network Administrator.	**No exceptions noted**
		5.2.3	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.	Inquired of the CFO and the Security Officer, that when an employee is terminated, HR notifies IT and an administrator will disable the terminated employee's access.	**No exceptions noted**
				Inspected the list of employees noting there were no terminated employees during the examination period.	**No exceptions noted**
		5.2.4	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.	Inquired of the Security Officer that 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.	**No exceptions noted**
				Inspected the Access Rights Review Form, noting that the review was performed by a member of senior management.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security.	5.1.4 (Repeat Control)	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.	Inspected the group policy settings indicating that a user ID and password is required to access non public information.	**No exceptions noted**
		5.3.1	Unique user IDs are assigned to individual users as part of the new user process.	Inspected the security policy noting that each employee will be assigned their own user ID.	**No exceptions noted**
				Inspected user listings for key system software, noting that unique user ID's were used.	**No exceptions noted**
		5.3.2	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.	Inspected the default domain policy indicating that passwords must be at least 6 characters and complex, lockout attempts and password history rules.	**No exceptions noted**
		5.1.9 (Repeat Control)	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.	Observed users gain access and be denied access with the dual factor software by supplying a user id, password, and a one-time system generated pin.	**No exceptions noted**
		5.3.4	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.	Observed a user gain entry to the IT Glue software, noting that multi-factor authentication is required to gain access. Inspected the multi-factor authentication log files noting that multi-factor authentication is setup for the respective users.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security.	5.1.2 (Repeat Control)	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.	Inspected a list of newly hired employees noting that the Director of Professional Services or the Leads Tool Engineer authorized access.	**No exceptions noted**
		5.2.1 (Repeat Control)	Requests to make changes to client users must be generated by the client via the ConnectWise ticket generation process, and must be approved by an authorized client employee.	Inspected a sample of tickets generated in ConnectWise by clients, noting that a request for new employee access was authorized by designated individuals.	**No exceptions noted**
				Observed a user access customer information using the ConnectWise system, noting a message occurs indicating those who are authorized to add/change/delete users.	**No exceptions noted**
		5.4.1	The ability to create or modify users and change user access privileges in ConnectWise is limited to authorized personnel.	Inspected a list of new users noting that new user was authorized by privileged individuals.	**No exceptions noted**
				Inspected a sample of tickets noting that changes to client employees were authorized by authorized individuals.	**No exceptions noted**
				Inspected the utility program noting that the ability to add/change or delete users are restricted to authorized technical services staff.	**No exceptions noted**
		5.2.3 (Repeat Control)	When employees are terminated, access authorities are disabled. HR notifies IT and an administrator will disable the terminated employee's access.	Inquired of the CFO and the Security Officer, that when an employee is terminated, HR notifies IT and an administrator will disable the terminated employee's access.	**No exceptions noted**
				Inspected an employee listing, noting there were no terminated employees during the examination period.	**No Exceptions noted**
		5.2.4 (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.	Inquired of the Security Officer that 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.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security.	5.5.1	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.	Inspected the keycard log noting the log included who used the card, when it was used and why.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.6	Logical access security measures have been implemented to protect against security threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	5.6.1	Users are authenticated by specific client software and user ID and passwords over encrypted transmissions.	Inquired of the Security Officer that users are authenticated by specific client software and user ID and passwords over encrypted transmissions.	**No exceptions noted**
				Inspected applicable the SSL certificates and connections noting that connections are encrypted and require a user login and ID to access the system.	
		5.6.2	Client users are authorized as part of the new client onboarding process, which requires authorization from specifically designated client employees. The client predetermines which individuals are authorized to approve new users, and those individuals are listed in the client profile section of ConnectWise.	Inquired of the Security Officer to verify that client users are authorized as part of the new client user process, which requires authorizations from specifically designated client employees, and that client predetermines which individuals are authorized to approve new users, and those individuals are listed in the client profile section of ConnectWise.	**No exceptions noted**
				Inspected a sample of new clients as part of the onboarding process to the ConnectWise system noting the proper client employee was setup as the primary contact to authorize changes.	
				Inspected a sample of tickets from the ConnectWise system noting the proper client employee authorized the user change.	
		5.6.3	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.	Inspected the firewall rules and email server properties noting that the configuration is set to allow only email from a third party email service.	**No exceptions noted**
		5.6.4	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.	Inquired of the Security Officer to verify that redundant firewalls are used and configured to prevent unauthorized access, and that the SonicWall firewall is integrated to ConnectWise and events automatically generate a ticket for research and resolution.	**No exceptions noted**
				Reperformed by attempting to reach the entity's servers through the firewall by using a utility, noting that the attempt failed.	
				Inspected the Hypervisor firewall and logging settings, noting that the system is configured to alert when specified events occur, and that a ticket is generated in ConnectWise.	
		5.6.5	Intrusion detection systems are used to provide continuous monitoring of the system and early identification of potential security breaches.	Inspected the configuration and a sample of a tickets generated from the anti-virus program noting that systems are being monitored for potential security breaches.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security.	5.7.1	The entity uses industry standard encryption technology, VPN software, or other secure communication systems for the transmission of private or confidential information over public networks, including user IDs and passwords. All traffic is encrypted.	Inspected site to site VPN software noting the connection is encrypted.	**No exceptions noted**
				Inspected firewall, VPN settings and log files noting that transmissions are encrypted.	**No exceptions noted**
				Inspected the secured website, where a client would access their own network, noting that the encryption key is managed by a third party provider.	**No exceptions noted**
		5.7.2	Entity policies prohibit the transmission of confidential or sensitive information over the Internet or other public communications paths unless it is encrypted.	Inquired of CFO and corroborated with the Security Officer, to verify that sensitive information transmissions are encrypted.	**No exceptions noted**
				Inspected an inventory of systems and noted encryption for each software is in place.	**No exceptions noted**
		2.2.3 (Repeat Control)	Each year, employees must reconfirm their understanding of and compliance with the information security policies by signing the Acceptable Use Agreement (AUA).	Inspected a sample of new employees noting there was a signed acceptable use agreement retained in the employee personnel file.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security.	5.8.1	Antivirus and antispyware programs are in place on all computers and servers, including scans of incoming email messages.	Inspected a sample of servers noting that antivirus and antispyware programs are in place.	**No exceptions noted**
		5.8.2	The Labtech management system monitors servers and computers for a wide variety of events, including infections and updates to antivirus and antispyware programs.	Inspected a sample of servers noting that the Labtech program is monitoring servers and computers for a variety of events including Infections and updates to system.	**No exceptions noted**
		5.8.3	Any events (such as virus detection or antivirus updates) generate a ticket for research and resolution.	Inspected the ConnectWise system noting that tickets were generated for virus detection.	**No exceptions noted**
		5.8.4	Email traffic is first routed to an offsite spam filter, and then routed to the CCR email server.	Inspected the firewall rules noting that access to email traffic comes from the spam filter.	**No exceptions noted**
		5.8.5	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.	Inquired of the Director of Professional Services that the ability to install, modify, and replace operating system and other system programs is restricted to authorized personnel.	**No exceptions noted**
		5.8.6	Access to superuser functionality and sensitive system functions is restricted to authorized personnel, as designated by the Director of Professional Services.	Inquired as to whether access of superuser functionality and sensitive system functions is restricted to authorized personnel, as designated by the Director of Professional Services.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC6.0	**Common Criteria Related to System Operations**				
CC6.1	Vulnerabilities of system components to security breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security.	4.1.1 (Repeat)	Network performance and system processing are monitored using system monitoring tools by staff 24 hours a day, 7 days a week.	Inquired of the Security Officer that automated monitoring systems are in place to monitor network performance and system availability.	**No exceptions noted**
		6.1.1	Network performance, system availability, and security incident statistics reports are reviewed by management.	Inspected a sample of weekly department meetings noting that network performance, system availability, and security incident statistics and were distributed to management as part of the meeting.	**No exceptions noted**
				Inspected a sample of minutes from Weekly Executive meetings noting a section regarding risk assessment and process/procedure that addressed system vulnerabilities.	**No exceptions noted**
		3.1.1 (Repeat)	Management performs on-going risk assessment to identify and manage risks that could affect the Company's ability to provide secure services to user entities.	Inspected a sample of minutes from Weekly Executive meetings noting a section regarding risk assessment and process/procedure.	**No exceptions noted**
				Inspected the Incident Response plan noting that a defined incident escalation process and notification mechanisms are included.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC6.2	security incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	6.2.1	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.	Inspected the ConnectWise Ticketing system for tickets of potential incidents.	**No exceptions noted**
		6.2.2	New customers are provided with instructions for communicating operational issues as part of CCR's onboarding process.	Inspected the onboarding template noting that instructions for communicating operational issues were included in the document.	**No exceptions noted**
		6.2.3	ConnectWise provides dashboards of outstanding tickets for management monitoring.	Inquired of management that open tickets get escalated to SI (systems integration) and are closed when completed, and that monitoring dashboards monitor all open tickets.	**No exceptions noted**
				Observed monitoring dashboards noting that tickets appear on the dashboard until closed.	**No exceptions noted**
		6.2.4	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.	Inquired of the Security Officer that when significant incidents are detected, a defined incident management process is initiated and the Director of Professional Services is notified.	**No exceptions noted**
				Inquired of the Security Officer of any security breeches during the examination period, noting there were none.	**No exceptions noted**
		6.2.5	The ConnectWise system provides dashboards for management monitoring of open tickets. Individuals assigned to resolving tickets document the final resolution on the ticket.	Inquired of the COO that open tickets get escalated to SI (systems integration) and are closed when completed. Monitoring dashboards monitor all open tickets.	**No exceptions noted**
				Observed monitoring dashboards noting that tickets appear on the board until closed.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
		6.2.6	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.	Inspected the Incident Response plan noting that a defined incident escalation process and notification mechanisms are included.	**No exceptions noted**
		6.2.7	Closed incidents are reviewed by management for appropriate resolution.	Inquired of the Security Officer that all closed incidents are reviewed by management for appropriate resolution. Observed the onscreen boards noting that tickets are tracked in the system until they are closed.	**No exceptions noted**
				Inspected closed tickets noting that management reviews them during the approval of employee's time.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC7.0	**Common Criteria Related to Change Management**				
CC7.1	The entity's commitments and system requirements, as they relate to security, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	7.1.1	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.	Inspected the written policy and change management procedures, noting performing application, system, hardware, software and network related changes were documented, as well as roles, responsibilities, and actions required to implement emergency changes.	**No exceptions noted**
		7.1.2	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.	Reperformed by initiatiating a ticket using the ConnectWise system noting a message occurs indicating those who are authorized to add/change/delete users.	**No exceptions noted**
				Inspected a sample of change requests tickets noting that authorized client users made the request.	**No exceptions noted**
		7.1.3	All change requests require completion of a Change Management Request form. The form includes the type of request, the impact, resources needed, and a risk assessment. The form requires approval of the Director of Professional Services or President.	Inspected a sample of change request forms with the type of sections and the supporting email noting the changes were properly approved.	**No exceptions noted**
		7.1.4	System change requests are evaluated to determine the potential effect of the change on security commitments and requirements throughout the change management process.	Inspected change request forms with the type of sections and the supporting email noting that the potential effect was evaluated and the changes were approved.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security.	7.1.4 (Repeat Control)	System change requests are evaluated to determine the potential effect of the change on security commitments and requirements throughout the change management process.	Inspected change request forms with the type of sections and the supporting email noting that the potential effect was evaluated and the changes were approved.	**No exceptions noted**
		7.1.3 (Repeat Control)	All change requests require completion of Change Management Request form. The form includes the type of request, the impact, resources needed, and a risk assessment. The form requires approval of the Director of Professional Services or President.	Inquired of the Director of Professional Services that all change requests require completion and approval of the Change Management Request forms by the Director of Professional Services.	**No exceptions noted**
				Inspected a sample of change request forms with the type of sections and the supporting email noting the changes were approved.	**No exceptions noted**
		7.2.1	The system monitoring tools scan all servers and computers and identify upgrades and patches needed.	Inquired of the system administrator and the Director of Professional Services to verify that system monitoring tools scan all servers and computers and identify upgrades and patches needed.	**No exceptions noted**
		7.2.2	Client requests for changes and system maintenance are entered into the ConnectWise system, which generates a ticket for research and resolution.	Inquired of the Director of Professional Services that client requests for changes and system maintenance are entered into the ConnectWise system and change requestors are kept informed.	**No exceptions noted**
				Inspected the ConnectWise system noting that an email field is available to email status information to user requests.	**No exceptions noted**
				Inspected the CCaRe portal noting that all ticket requests are available for review.	**No exceptions noted**
				Observed monitoring boards noting that tickets appear on the board until closed.	**No exceptions noted**
		2.6.2 (Repeat Control)	Changes to system components that may affect systems processing performance, availability, and security require the approval of the Security Officer.	Inspected change request forms with the type of sections and the supporting email noting the changes were approved.	**No exceptions noted**
		7.2.3	The Security Officer reviews and approves the architecture and design specifications for new systems development and acquisition to ensure consistency with the entity's related security policies.	Inspected change request forms with the type of sections and the supporting email noting the changes were approved.	**No exceptions noted**

Criteria No.	Criteria Description	Control No.	CCR Controls	Test by Auditor	Results
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security.	7.3.1	Management performs on-going risk assessment to identify and manage risks that could affect the Company's ability to provide secure services to user entities. During the on-going risk assessment process, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are initiated based on the identified needs.	Inspected a sample of minutes from Weekly Executive meetings noting a section regarding risk assessment and process/procedure.	**No exceptions noted**
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security commitments and system requirements.	7.1.3 (Repeat Control)	All change requests require completion of 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.	Inspected change request forms noting both with the type of sections and the supporting email noting the changes were approved.	**No exceptions noted**
		7.4.1	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.	Inspected a sample of employees noting they signed the "Acceptable Use Agreement" which prohibits unauthorized system changes.	**No exceptions noted**
		7.4.2	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.	Inquired of the Director of Professional Services that procedures exist to provide that emergency changes are documented and authorized timely. Inquired of the Director of Professional Services that no emergency changes existed during the examination period.	**No exceptions noted**