CONNECTWISE, LLC

ConnectWise Continuum System

SOC 3® System and System and Organization Controls (SOC) for Service Organizations

Report throughout the period of May 1, 2020 through October 31, 2021
# Table of Contents

I. Report of Independent Service Auditor ............................................................................................................... 1  
II. ConnectWise LLC’s Assertion .......................................................................................................................... 3  
III. Management of ConnectWise’ Description of its Continuum System ............................................................. 4  
   A. Scope and Purpose of the Report ......................................................................................................................... 4  
   B. Company Overview and Background .................................................................................................................. 4  
   C. Principal Service Commitments and System Requirements .................................................................................. 5  
   D. Components of the System Used to Provide the Services ............................................................................... 5  
   E. Policies and Procedures ....................................................................................................................................... 6  
   F. User Entity Controls ......................................................................................................................................... 10  
   G. Subservice Organizations ................................................................................................................................... 11
I. Report of Independent Service Auditor

To: Management of ConnectWise, LLC

Scope
We have examined ConnectWise LLC’s (the “Company”) accompanying assertion titled ConnectWise LLC’s Assertion (the “Assertion”) that the controls within ConnectWise LLC’s Continuum System were effective throughout the period May 1, 2020 to October 31, 2020 (the “Specified Period”), to provide reasonable assurance that ConnectWise’ service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Confidentiality, and Privacy (“applicable Trust Services Criteria”) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

ConnectWise uses Amazon Web Services as a subservice provider for hosting of the production infrastructure system and associated physical security and infrastructure support. The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled Management of ConnectWise’ Description of its Continuum System, under the section Subservice Organizations, can be achieved only if complementary subservice organization controls assumed in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to the controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled Management of ConnectWise’ Description of its Continuum System, under the section User Entity Controls, can be achieved only if complementary user entity controls contemplated in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company. 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.

Service organization’s responsibilities
ConnectWise is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company’s service commitments and system requirements were achieved. ConnectWise has provided the accompanying assertion titled ConnectWise LLC’s Assertion about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor’s responsibilities
Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.
Our examination included:

- obtaining an understanding of the system and the service organization’s service commitments and system requirements;
- assessing the risks that the controls were not effective to achieve the Company’s service commitments and system requirements based on the Applicable Trust Services criteria; and
- performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company’s service commitments and system requirements based on the Applicable Trust Services Criteria;

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

**Inherent limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

**Opinion**

In our opinion, ConnectWise’ assertion that the controls within the Continuum System were effective throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Atlanta, Georgia
February 24, 2021
II. ConnectWise LLC’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over ConnectWise LLC’s (the “Company”) Continuum System (the “System”) throughout the period May 1, 2020 to October 31, 2020 (the “Specified Period”), to provide reasonable assurance that the Company’s service commitments and system requirements relevant to Security, Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Privacy (the “Applicable Trust Services Criteria”) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The Company’s objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria are specified in Section III titled Management of ConnectWise’ Description of its Continuum System.

ConnectWise uses Amazon Web Services as a subservice provider for hosting of the production infrastructure system and associated physical security and infrastructure support. Certain AICPA Applicable Trust Services Criteria specified in the section titled Management of ConnectWise’ Description of its Continuum System, under the section Subservice Organizations, can be achieved only if complementary subservice organization controls assumed in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company. Management’s assertion includes only the controls of the Company and excludes the controls performed by the subservice organization.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, Management of ConnectWise’ Description of its Continuum System under the section User Entity Controls can be achieved only if complementary user entity controls contemplated in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company. Management’s assertion includes only the controls of the Company and excludes the controls performed by User Entities.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.
III. Management of ConnectWise’ Description of its Continuum System

A. Scope and Purpose of the Report

This report describes the control structure of ConnectWise (the “Company”) as it relates to its ConnectWise Continuum Services (the “System”) for the period of May 1, 2020 to October 31, 2020 (the “Specified Period”) for the Security, Confidentiality, and Privacy Trust Services Categories (the “Applicable Trust Services Criteria”) as set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

ConnectWise is an IT software company, powering Technology Service Providers (TSP) to achieve their vision of success in their as-a-service business with intelligent software packages, expert services, and vast eco-system of integration. ConnectWise has unmatched flexibility which caters profitable long-term growth to TSPs.

ConnectWise develops and distributes a business management platform. The company offers a suite of applications that includes an integrated customer relationship management (CRM) solution, help desk and customer service applications, project management, finance and billing systems, and a workflow automation solution. ConnectWise software caters to information technology services, system integration, software development, professional services, and telecommunications sectors. The company was founded in 1982 and is based in Tampa, Florida.

Overview of the Continuum Systems

Continuum offers two different products: Continuity 247 and R1Soft. Continuity247 (C247) is a backup and disaster recovery application developed and managed by our team in Houston, TX. Continuum also sells a R1Soft packaged software product, usually purchased by partners to manage customer backups either locally or in the cloud.

C247 is our fully managed backup and disaster recovery platform. Designed to access client backup data quickly while maintaining recovery points offsite, C247 combines a local, onsite appliance with offsite cloud storage to provide a comprehensive hybrid backup solution.

Should an event occur where the local servers and desktops or the backup appliance become unavailable, virtual instances of protected machines can be spun up in the cloud to ensure business continuity. C247 is fully managed by Continuum’s NOC technicians 24x7x365. Customers can also choose to self-manage.

Key Features

- Self-service flexibility and granular file and folder browsing & recovery
- Self-service virtualization of individual machines on appliance and cloud
- Bare-metal resources for Windows servers
- Automatic data replication between multiple datacenters
- Granular scheduling of backup and retention policies
- Block-level encryption
• Industry standard AES-256 encryption (at rest and in transit)

C247 Components
• Agent
• Site SBM
• Cloud SBM
• Resource Manager
• Consolidation Manager
• FTPS Server

C. Principal Service Commitments and System Requirements

Continuum is committed to the security, privacy, and accessibility of your data. We strive to be as transparent as possible with our data collection and usage practices, with a goal of providing best-in-class products, services, and web experiences for users. We understand that individual rights, requirements, and policies vary significantly across the globe, as well as for various users and audience members.

Our commitment to data protection and privacy can be summarized in three key areas which are outlined below:

Your data is protected
We treat the security of your data as a top priority and take precautions to protect your data from accidental loss, unwanted exposure, or theft. Our products and web properties are designed to adhere to industry guidelines and best practices for encryption, storage, and usage.

You understand exactly how your data is used
Continuum collects and processes data within our products and across web properties to provide you with valuable and rich digital experiences. We strive for total transparency about the usage and collection of your data, and Continuum will never sell, share, or leverage your data for anything other than legitimate business purposes without your express consent.

You have control over your data
We believe the process of accessing and collecting your data should be as straightforward as possible. We are currently working to streamline and optimize a complete process through which you can gain access to any data stored or processed by Continuum.

D. Components of the System Used to Provide the Services

Continuum has four offices, three in the United States (Boston, MA; Cranberry, PA; and Houston, TX) and one in Mumbai, India. Continuum also maintains co-location space at a datacenter in Boston, MA that houses Continuum’s portal and an on-site data center in Houston, TX that houses Continuum’s backup and recovery products. In addition, Continuum has a hot backup data center in Lenoir, NC that is activated only when Continuum’s itsupport247.net portal is unavailable for more than 15 minutes.

Additionally, Continuum leverages AWS’ cloud-based datacenters. Continuum uses CloudWatch and CloudTrail logs for AWS monitoring. For access control of its AWS instances, Continuum uses AWS IAM. Continuum also uses Security Groups and VPC features to establish boundaries and restrict logical access.

While Continuum does offer VPN access to offices, such access is reserved for administrative users. Administrative users maintain and manage the local networks and systems and maintain the development, testing, and production systems that Continuum’s customers and partners use. While Continuum maintains direct VPN connections between offices in India and the US to facilitate call center routing and other communication activities, most communication and collaboration among Continuum employees occurs predominately via cloud services (e.g., e-mail and calendaring, video conference, written collaboration), which are accessible through encrypted (SSL/TLS) web connections.
All Continuum edge routers are maintained and managed by a network administration team based in the US (Boston, MA) and Mumbai, India. Continuum’s directory services and tech support are also managed by a global IT team, based in Boston and Mumbai.

E. Policies and Procedures

Continuum management has developed and communicated policies and procedures to all corporate employees and contractors to secure systems and facilities and reduce the risk of data loss, compromise, or breach. Changes to these policies and procedures are performed annually and are authorized by senior management.

- **Acceptable Use**: The purpose of this policy is to set expectations that users are required to adhere to regarding the proper use and protection of all information systems.
- **Third Party Vendor – Data Protection**: The purpose of this policy is to ensure vendors maintain adequate risk management programs to protect customer information.
- **Acceptable Encryption**: The purpose of this policy is to require strong encryption controls to protect the company’s information in transit and at rest to ensure confidentiality and integrity.
- **Acquisition Assessment**: The purpose of this policy is to establish information security responsibilities in the event of a corporate acquisition and define the minimum-security requirements of an information security acquisition assessment.
- **Anti-Virus**: The purpose of this policy is to safeguard all devices owned by the Company from malicious code.
- **Data Backup**: The purpose of this policy is to ensure the availability of data and ensure business continuity in the event of an accidental deletion or corruption of data.
- **Data Retention and Records**: The purpose of this policy is to ensure that all information is retained and disposed of in accordance with business, legal, and regulatory requirements.
- **Security Credentials Management**: The purpose of this policy is to ensure the confidentiality and integrity of databases where credential information is stored.
- **Destruction of Electronic Media**: The purpose of this policy is to establish a standard for the proper disposal of media containing electronic data and prevent unauthorized disclosure of the information.
- **Information Security Risk Assessment**: The purpose of this policy is to perform periodic information security risk assessments to ensure risks are identified, mitigated, and communicated in a timely manner.
- **Information Sensitivity**: The purpose of this policy is to define the classification of the Company's information and provide guidelines for the management of information to ensure it is protected from unauthorized and unintentional access, use, and disclosure in accordance with its level of sensitivity.
- **Password**: The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of password changes.
- **Patch Management**: The purpose of this policy is to define patch management practices including acquiring, testing, and installing patches of software for existing applications.
- **Physical Security for Information Resources**: The purpose of this policy is to control physical access to information resources. This policy sets forth the rules for establishing, controlling, and monitoring physical access to information resources.
- **Remote Access**: The purpose of this policy is to ensure adequate security measures while accessing information from remote locations or mobile devices.
- **Network Security**: The purpose of this policy is to ensure that access to ConnectWise’s networks are managed and controlled to protect information and information systems.
- **Secure Application Development**: The purpose of this policy is to ensure business applications are written with secure coding standards to protect the confidentiality and integrity of information.
- **Server Security**: The purpose of this policy is to establish standards for the base configuration of internal servers that are owned and/or operated by ConnectWise.
- **Change Management**: The purpose of this policy is to manage changes made to information assets, including network infrastructure and applications, by ensuring that changes to the IT environment are made in a controlled manner.

- **Access Control**: The purpose of this policy is to ensure the confidentiality and integrity of information and to grant and revoke information access in a timely manner in accordance with business requirements.

- **Incident Response**: The purpose of this policy is to define steps to quickly recover from any type of security incident and minimize the business impact, while maintaining business continuity.

- **Information Security Continuity**: The purpose of this policy is to ensure the continuity and security of operations in the event of a disaster.

- **Information Security Compliance Policy**: The purpose of this policy is to ensure compliance with relevant laws and regulations.

- **Asset Management**: The purpose of this policy is to maintain documented asset management guidance and to achieve and maintain appropriate protection of company assets.

- **Vulnerability Management**: The purpose of this policy is to maintain a documented vulnerability management program, which guides authorized personnel in the performance of information security vulnerability assessments to identify vulnerable areas. Critical vulnerabilities are required to be remediated within 30 days of identification and high vulnerabilities are required to be remediated within 60 days of identification. Additionally, penetration tests are required to be performed bi-annually to identify vulnerabilities present in the organization.

**Procedures**

1. **Change Control**

   It is Continuum’s policy to ensure that all significant, non-routine changes to information assets, information processing facilities, infrastructure components, and application environments are documented, reviewed, and approved by the Change Advisory Board (CAB) and/or designated approvers. Significant, non-routine changes to information or IT environments include, but are not limited to:

   a. Implementation of added resources or functionality
   b. Modification to existing IT resources or functionality
   c. Removal or disposal of existing IT resources or functionality
   d. Interruption of service

   Server and operating systems are required to be hardened as described in the IS Policy. The Information Security Team runs scans to ensure devices are hardened in compliance with Continuum policy.

   All changes go through a process where there is segregation of duties between the application, development, promotion, and verification. Additionally, changes are tested prior to deployment, and the asset inventory is updated after every change. There are named and identified resources for each application area, and changes are required to be communicated to relevant personnel with operational instructions, as applicable.

2. **Penetration Testing**

   Continuum’s Security team performs web application penetration tests twice per year (bi-annually), and external web application penetration tests are performed annually.

   Continuum conducts one full external penetration test and three to four maintenance tests per year, along with ongoing static (black box) testing of all product components. The Information Security team performs penetration testing bi-annually to identify vulnerabilities present in the organization. Risks identified during these tests are ranked in order of severity of the system to intrusion attacks. Resolution activities for the identified risks are assigned to the appropriate departments and tracked by the Information Security team to ensure that the risks are addressed.
3. **Business Recovery Planning**

   Continuum runs virtualized servers in the primary Continuum datacenter. The servers are backed up hourly and snapshotted once per day. The IT and DevOps teams maintain and receive status alerts for hourly replication jobs and daily snapshots of systems and information. Five server images are always backed up for production. In the event of an outage at the main datacenter that lasts more than 15 minutes, the Continuum Control Portal is transferred to a backup co-location facility located in a different geographical region. During an outage of the main portal, the new portal is called the Control DR Portal. The Control DR Portal has been provisioned for disaster recovery purposes after a disaster has been declared for the primary IT Support 24/7 Control Portal. This allows Continuum’s partners to perform a limited set of functions as listed below until the primary portal is operational and available for use.

   - Partners can access the Quick Access servers and desktops
   - Partners can remotely access the devices shown in Quick Access using LogMeIn
   - Two-factor authentication
   - Partner Freezing Checks – Ability to confirm locked partners cannot access sites
   - LogMeIn Rescue + Mobile
   - Online support (using LogMeIn Rescue)
     - Only the new session option is made available

4. **Talent Management Practices**

   The Company strives to attract and maintain the most skilled, talented, and conscientious employees. Employees are committed to maintaining the confidentiality, integrity, and availability of customers’ resources and data.

   **Onboarding and Offboarding**

   Continuum’s hiring processes are defined in The Manager’s Tool-Kit, an extensive guide that describes the responsibilities and processes for new hire recruiting, interviewing, engagement, and onboarding. All applicants move through several steps and meet with several current employees in a process to determine their competencies, experience, and organizational fit. Applicants must also complete a background check as a condition of employment.

   Employees are granted access to Continuum’s systems and data as it relates to their job function. The HR department and the employee’s manager approve access and make a ticket request to the IT department, which grants the access requested. IT holds regular review meetings to ensure that employee access fits with employees’ roles and responsibilities.

   The Manager’s Tool-Kit also defines processes for employee termination. All managers must follow pre-determined checklists for both voluntary and involuntary terminations. During the termination process, the manager sends a ticket to IT to remove all access and disable the user’s accounts. For voluntary terminations, the IT department removes access and disables the account within 24 hours. For involuntary terminations, IT will remove access and disable the account during the termination process. All disabled accounts are deleted within 90 days.

   **User Training**

   Continuum requires that all employees complete annual security and job skills training. Depending on the job function, employees may receive more focused training that covers specific skills. For example, all developers must complete OWASP training annually in addition to the standard security training requirements. ConnectWise is a global company; as such, training is delivered both online and in face-to-face sessions.
5. **Oversight by the Board of Directors**
   ConnectWise Board of Directors oversee Continuum’s activities. The Board of Directors is comprised of six members who meet with the Executive Team every quarter. The Board has the following responsibilities with respect to Continuum:
   - Review Continuum’s strategic and tactical plans to ensure that the annual business plan goals are aligned.
   - Monitor progress against the business plan and ensure adequacy of resources, including cash and human capital, using key metrics.
   - Ascertain that Continuum is compliant with all laws, regulations, etc. that govern the operations of the business.
   - Review financial performance budget vs. actual with an understanding of underlying internal controls.
   - Meet annually with the auditors to discuss the audited financial statements and the results of the audit.

6. **Network Systems Development and Maintenance**
   Continuum employs a formal development life cycle methodology governing the development, acquisition, implementation, and maintenance of its information systems and related technology. Network system architecture and design specifications are reviewed and approved. Continuum uses special purpose software to monitor servers, operating systems, and other major system components. In addition, manufacturer notifications are subscribed to for all hardware and software components. Current versions of all software and patches are maintained.
   Continuum notifies customers well in advance of any scheduled system maintenance and performs routine system maintenance as scheduled. The disaster recovery data center (C247) is used should the need arise to perform emergency or non-routine maintenance on the system.

7. **Intrusion Detection and Incident Response**
   Best practice intrusion detection systems (IDS) and intrusion prevention systems (IPS) are implemented across the organization. Mechanisms exist to detect intrusions and denial of service attacks and to initiate appropriate responses. Fortinet and Palo Alto appliances are used for intrusion prevention and detection.
   Users of the Continuum service are provided with instructions on how to communicate potential security breaches via a monitored e-mail address. Continuum engages a third-party SIEM and security operations center service to capture and correlate logs from servers throughout the company and provide alerting.

8. **System Monitoring**
   Continuum utilizes an IT infrastructure monitoring system, anti-virus system, and endpoint protection system to monitor the devices that support the products and services in the scope of this report. A security information and event management system monitors the security events identified by those systems to correlate issues identified across the infrastructure.

9. **Control Monitoring**
   The Information Security team performs internal audit activities to ensure that controls are operating as intended. Some controls are evaluated monthly while others are examined either quarterly, bi-annually, or annually, depending on the frequency at which the control is performed. The internal audit process includes input from various departments, and the findings are reported to relevant personnel for remediation in accordance with pre-defined timelines.

10. **Risk Assessment**
    The information security risk assessment consists of three components:
    - Risk Identification – Document the assets, threats, vulnerabilities, impact, existing controls, and risk statement for the IT resources that will be covered by the assessment.
    - Risk Assessment – Document the degree of impact/severity, likelihood, and risk value of the risks identified for the IT resources that will be covered by the assessment.
• Risk Treatment
  o Select controls to manage the identified risks.
  o Conduct a gap assessment of the selected controls to document their existing implementation or plans for new/additional controls to manage the risk.

A Corporate Compliance Policy is maintained by management, which defines the responsibilities for evaluating risk to the organization and determining safeguards to mitigate or reduce those identified risks to an acceptable level. A risk assessment is conducted in the event of a major change to the environment, and at least annually.

Continuum regularly reviews the risks that may result in impairment of the Security, Confidentiality, or Privacy criteria as set forth in the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. The Information Security team assesses risks on an ongoing basis. This is completed through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment. An IT strategic plan is developed annually by the CISO and the plan is communicated to and approved by senior management. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed. Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Continuum’s security policies. Changes in security threats and risks are reviewed, and updates to existing control activities and information security policies are performed, as necessary.

F. User Entity Controls

Continuum System’s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company’s service commitments and system requirements to be achieved based on the applicable Trust Services Criteria solely by the Company. ConnectWise’s control policies and procedures were designed with the assumption that certain controls as defined below, would be in place and in operation at the sub-service organization and user entities. Sub-service organization controls and user entity internal controls must be evaluated, taking into consideration ConnectWise controls and their own internal controls. ConnectWise’s management does not make any representations regarding responsibility related to, or provide any assurance in regard to any such internal control or regulatory requirements for which the client must assess or comply.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity control responsibilities as defined in the following, have been implemented and are operating effectively:

• User entities are responsible for informing ConnectWise of any regulatory issues that may affect the services provided by Continuum System to the user entity.
• User entities are responsible for understanding and complying with their contractual obligations to Continuum System.
• User entities are responsible for determining whether Continuum System’s security infrastructure is appropriate for its needs and notifying Continuum personnel of any requested modifications.
• User entities are responsible for notifying the company personnel, in a timely manner, when changes are made to technical, billing, or administrative contact information.
• User entities are responsible for ensuring that appropriate individuals have the requisite training on Continuum System software.
• User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with the company’s systems.
• User entities are responsible for ensuring that user IDs and passwords are only assigned to authorized individuals and that the roles assigned to the user accounts are appropriate.
User entities are responsible for the administration of user access for Continuum System applications.

User entities are responsible for implementing a security infrastructure and practices to prevent unauthorized access to their internal network and to limit threats from connections to external networks.

User entities are responsible for immediately notifying the company personnel of any actual or suspected information security breaches, including compromised user accounts.

User entities are responsible for responding to alert notifications.

G. Subservice Organizations

ConnectWise uses Amazon Web Services for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control functions performed by AWS are critical to achieving the Company’s service commitments and system requirements based on the applicable trust services criteria:

- Physical security of the datacenters hosting the in-scope applications,
- Environmental controls, around the backup processes at the datacenters hosting the in-scope applications to support the disaster recovery processes, and
- Processes to ensure the secure destruction of decommissioned equipment.

ConnectWise has deployed the following controls to help monitor the subservice organization:

- On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.