CONNECTWISE, LLC

ConnectWise Bright Gauge

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

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

I. **Report of Independent Service Auditor** ................................................................. 2

II. **ConnectWise LLC’s Assertion** .................................................................................. 4

III. **Management of ConnectWise’ Description of its Bright Gauge 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. ConnectWise Control Environment ............................................................. 5
    F. Policies and Procedures .................................................................................. 8
    G. User Entity Controls ..................................................................................... 10
    H. 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 Bright Gauge 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 Bright Gauge 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 Bright Gauge 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 Bright Gauge 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”) Bright Gauge 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 Bright Gauge 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 Bright Gauge 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 Bright Gauge 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 Bright Gauge System

A. Scope and Purpose of the Report

This report describes the control structure of ConnectWise (the “Company”) as it relates to its ConnectWise Bright Gauge (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.

Bright Gauge is an IT documentation system managed by ConnectWise. It has a versatile dashboard that hosts the most advanced documentation solution in the industry and displays the numbers you need to see from your external platforms.

Founded in 2018 and acquired by ConnectWise in 2019, Bright Gauge is a Software as a Service (SaaS) system that includes controls designed to meet the applicable Trust Services Criteria. Management is responsible for the identification of risks associated with the system of controls, and for the design and operation of controls intended to provide reasonable assurance that the applicable Trust Services Criteria would be met.

Bright Gauge System Overview

- **Documentation** – Whether you prefer to work off customizable templates or build your knowledge base from the ground up, everything you need to customize your documentation experience with Bright Gauge is at your fingertips.

- **Comprehensive Dashboard** – Bright Gauge links your critical information together across companies, contacts, and assets, enabling organizations to deliver seamless customer experiences from a single pane-of-glass view.

- **Customized Templates** – Bright Gauge eases the documentation process with the use of customized templates.

- **VOIP Integrations** – With Ring Central and Jive VoIP integrations, on-screen prompts deliver all the information your techs need to provide a seamless and consistent customer support experience.
C. Principal Service Commitments and System Requirements

ConnectWise takes security very seriously. ConnectWise looks at security as a dynamic threat and will continue to work to optimize security for our partners and community. ConnectWise regularly conducts penetration tests that are performed by both internal and external ethical hackers and we run vulnerability assessments on our systems and products on a consistent basis.

ConnectWise products are subject to multiple layers of security from design through testing and into operations. Products designs are aligned with security best-practices and undergo security testing prior to release and regularly in production. In addition, ConnectWise developer’s complete security training on an annual basis at a minimum.

Security commitments to user entities are documented and communicated in Terms and Conditions and other partner agreements, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Use of encryption technologies to protect partner data stored and in transit
- Role-based access controls to limit user access to sensitive data

ConnectWise’s management establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated through ConnectWise’s system policies and procedures, system design documentation, and contracts with partners. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

D. Components of the System Used to Provide the Services

Bright Gauge is a cloud-based SaaS application that is hosted solely in AWS. Partners connect to Bright Gauge using a web browser.

ConnectWise automates the network security services for their cloud environment. The production infrastructure resides within AWS data centers in multiple availability zones. Partners only have access to their instance. Remote access to the production network is granted via encrypted VPN client requiring multi-factor authentication. A DMZ is implemented in the cloud-hosted environment to limit inbound traffic from the internet to externally facing production servers while restricting direct access to back-end services.

The ConnectWise internal network is protected from public internet traffic via stateful inspection firewalls managed by corporate I.T. personnel. These firewalls are configured to deny all traffic and only allow specific services to a specific destination. Access to administer the firewalls is restricted to personnel in the Cloud Infrastructure group and is commensurate with their job responsibilities. Custom rules are added that govern the allowed inbound traffic to ConnectWise resources. All other inbound traffic is denied. Rules can be modified as needed and new rules are automatically enforced for all existing and future resources.

Encrypted communications are utilized to protect remote internet sessions to the ConnectWise applications and internal network. Encryption is used to ensure the privacy and integrity of the data being passed over the public network.

E. ConnectWise Control Environment

The control environment at ConnectWise begins at the highest level of the Company. The Board of Directors includes members independent of the daily operations and is established to provide strategy and oversight to the operational leaders. Executive and senior leadership play important roles in establishing the Company’s core values and tone at the top. Every employee is provided with the Company’s Code of Business Conduct and Ethics, which sets guiding principles.
ConnectWise is committed to protecting its customer’s data and maintaining compliance with applicable regulatory requirements. This is demonstrated by a consolidated Risk Management Program to enable the identification and assessment of risks relating to company objectives. ConnectWise policies and procedures outline the required guidance for operation and information security that support ConnectWise environments, acceptable use of mobile devices, and access to data content and network devices. ConnectWise employees are required to review applicable policies and procedures, as updated from time to time. Evidence of compliance with the training on ConnectWise policies is executed and retained by the Legal, Talent and University teams.

ConnectWise has setup a hotline for employees to report any misconduct or violation of ConnectWise policies, practices, rules, requirements, or procedures. Any material violation to the Company Code of Business Conduct and Ethics or any other similar policies are appropriately handled accordingly which may include disciplinary action or termination of employment.

ConnectWise has implemented a formal Executive Information Security Council that is responsible for steering the information security program, monitoring the design, and operating effectiveness of that program, and addressing significant information security risks, issues, and exceptions.

ConnectWise has a dedicated information security team responsible for ConnectWise’ s overall security strategy, including identifying and implementing security practices, policies and solutions, and recommending best practices for infrastructure and application security. ConnectWise CISO serves as a thought leader within the company, keeping colleagues and the executive leadership team educated on all matters related to security. The ConnectWise Security team has established an information security framework and regularly reviews and updates the security policy, provides security training to employees, and performs application security reviews. These reviews assess the availability, confidentiality, and integrity of data, as well as conformance to the information security policy.

The ConnectWise organizational structure provides a framework for planning, executing, and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

Additional aspects of ConnectWise control environment include the following:

**Personnel Management**

The Company follows a structured on-boarding process to assist new employees as they become familiar with ConnectWise products, processes, systems, policies, and procedures. ConnectWise performs a formal evaluation of the appropriate resourcing and staffing to align employee qualifications with the entity’s business objectives to support the achievement of the entity’s business objectives. Appropriate feedback is given to the employee on strengths and growth areas during the annual performance review process. Employee strength and growth evaluations are shared by the employee’s manager with the employee.

An access request form is completed for personnel as a component of the hiring procedures prior to granting system access. The form is authorized by the appropriate supervisor or manager and documents the equipment provided and types of systems access required. The completed form is provided to the corporate IT team to provision the requested level of access. Employees are limited to system resources that they require to perform their job responsibilities.

A similar form is completed as a component of the termination procedures to collect equipment assigned to the employee and to revoke systems access. The completed form is distributed to corporate I.T. So that systems access can be revoked within 24 hours of employees exit.

**Risk Assessment**

A Risk Assessment Policy is maintained by management that defines the responsibilities and management for evaluating risk to the organization and determining safeguards to mitigate or reduce those identified risks to an acceptable level. Risk assessment is conducted annually or in the event of a major change in the environment. Risk assessment activities include identification of risk and vulnerabilities, prioritize risk by assigning a risk score and the risk as per their criticality.
ConnectWise’s recognition of risks that could affect the organization’s ability to provide reliable services for its user entities is implicit, rather than explicit. Management’s involvement in the daily operations allows them to learn about risks through direct personal involvement with personnel and outside parties.

Identified risks are documented and ranked in the annual risk register. The risk register includes rankings based on a combination of impact and likelihood, identified mitigation activities, and mitigation owners.

**Control Monitoring**

Management performs monitoring activities to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

KRI is performed by ConnectWise Information Security Team which is a part of Internal Audit and is performed monthly. Some controls are evaluated monthly while some are examined on a Quarterly/Bi-annual/Annual basis as per the duration defined. This internal audit involves input from HR, Engineering, and IT Teams.

After the audit, the result of the audit is communicated to the relevant stake holders so adequate step are taken to mitigate the findings of the Audit.

ConnectWise’s management obtains and reviews the annual Service Auditor’s reports and for the subservice organization to monitor and evaluate the adequacy and effectiveness of controls in place at the sub-service organization.

**Communication System**

Management is involved with day-to-day operations and can provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. Management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

**Data Security**

The system of information security controls was designed to protect specific client contact information, server location, and access credentials. ConnectWise products and services operate with a defined hierarchy of access control requirements.

- Partners can only see their own information.
- Clients can only see their own information.

Data is handled in accordance with the Data Handling Policy present in the IS Policy. As per the Data Classification Policy, the following classifications are maintained: Sensitive Information, Confidential Information, Internal, and Public Information. Each type of information has their own exposure level.

The nature and purpose of processing customer’s personal data is to:

1. Provide the service.
2. Provide technical administration and customer support.
3. Respond to inquiries.
4. Send important notices, such as communications about purchases and changes to terms, conditions, and policies.
5. Process payments for purchases made.
6. Deliver products and services purchased or requested.
7. Manage use of the service.
8. Enforce terms of service.
F. Policies and Procedures

ConnectWise 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**

Standard operating procedures (SOPs) are documented for automated and manual procedures involved in the operation of the SaaS platform. Along with SOPs, management has identified and put into effect actions needed to affect those standards. Control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently.

Documented information security policies and procedures are in place to guide IT and operations personnel in information security administration processes, including, but not limited to Acceptable usage, access provisioning, Password management, Change management, Incident Response, Network Security, Database Security, Asset Management, Information Security Risk Assessment, Vendor Security Risk Management and data retention and classification. The policies are made available via the intranet and personnel are required to acknowledge their acceptance. A security awareness program is administered annually, and completion is compulsory.

**Incident Response**

Documented escalation procedures for reporting incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints. IT personnel utilize an automated ticketing system to document system incidents, response, and resolution. The ticketing system provides the means to document, track, notify, and escalate incidents that are reported. Incidents are classified based on urgency and include an initial description of the incident which can be linked to an impacted asset (e.g., a server). Incident tickets also include a history of the steps followed to resolve the particular issue.

**Communication Systems**

Management is involved with day-to-day operations and provide personnel with an understanding of their individual roles and responsibilities. This includes providing the necessary training to ensure that personnel understand how their daily activities and roles relate to the overall support of services. Management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

**Risk Assessment**

A Risk Assessment Policy is maintained by management that defines the responsibilities and processes for evaluating risks to the organization and determining safeguards to mitigate or reduce those identified risks to an acceptable level.

Bright Gauge’s recognition of risks that could affect the organization’s ability to provide reliable services for its user entities is generally implicit, rather than explicit. Management’s involvement in the daily operations allows them to learn about risks through direct personal involvement with personnel and outside parties.
Identified risks are documented and ranked in the risk register. The risk register is updated at least annually and includes rankings based on a combination of impact and likelihood, identified mitigation activities, and mitigation owners.

**Access Requests and Access Revocation**

An access request form is completed for personnel as a component of the hiring procedures prior to granting system access. The form is authorized by the appropriate supervisor or manager and documents the equipment provided and types of system access required. The completed form is provided to the corporate IT team to provision the requested level of access. Employees are limited to system resources that they require to perform their job responsibilities.

A similar form is completed as a component of the termination process to collect equipment assigned to the employee and to revoke system access. The completed form is distributed to corporate IT so that system access can be revoked.

**G. User Entity Controls**

Bright Gauge’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. Therefore, each user entity’s internal control must be evaluated in conjunction with the Company’s controls and related testing detailed in Section IV of this report, considering the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

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:

- Informing Bright Gauge of any regulatory issues that may affect the services provided by Bright Gauge to the user entity.
- Understanding and complying with their contractual obligations to Bright Gauge.
- Determining whether Bright Gauge’s security infrastructure is appropriate for its needs and notifying Bright Gauge personnel of any requested modifications.
- Notifying Bright Gauge personnel, in a timely manner, when changes are made to technical, billing, or administrative contact information.
- Ensuring that appropriate individuals have the requisite training on Bright Gauge software.
- Ensuring the confidentiality of any user IDs and passwords assigned to them for use with Bright Gauge’s systems.
- Ensuring that user IDs and passwords are only assigned to authorized individuals and that the roles assigned to the user accounts are appropriate.
- Administration of user access for Bright Gauge applications.
- Implementing a security infrastructure and practices to prevent unauthorized access to their internal network and to limit threats from connections to external networks.
- Notifying Bright Gauge personnel of any actual or suspected information security breaches, including compromised user accounts.
- Responding to alert notifications.
H. 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.