



A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Summit Hosting LLC

Year:
2026



SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2025 to June 30, 2026

Table of Contents

SECTION 1 ASSERTION OF SUMMIT HOSTING LLC MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT	3
SECTION 3 SUMMIT HOSTING LLC'S DESCRIPTION OF ITS IT SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2025 TO JUNE 30, 2026	6
OVERVIEW OF OPERATIONS.....	7
Company Background	7
Description of Services Provided	7
Principal Service Commitments and System Requirements.....	12
Components of the System.....	13
Boundaries of the System.....	19
Changes to the System Since the Last Review.....	19
Incidents Since the Last Review	19
Criteria Not Applicable to the System	19
Subservice Organizations.....	19
COMPLEMENTARY USER ENTITY CONTROLS.....	29

SECTION 1

ASSERTION OF SUMMIT HOSTING LLC MANAGEMENT

ASSERTION OF SUMMIT HOSTING LLC MANAGEMENT

July 17, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Summit Hosting LLC's ('Summit' or 'the Company') IT Services System throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Summit's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Summit Hosting LLC's Description of Its IT Services System throughout the period July 1, 2025 to June 30, 2026" and identifies the aspects of the system covered by our assertion.

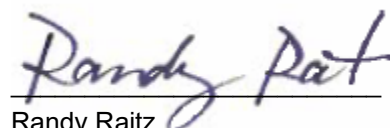
We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Summit's service commitments and system requirements were achieved based on the trust services criteria. Summit's objectives 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 presented in "Summit Hosting LLC's Description of Its IT Services System throughout the period July 1, 2025 to June 30, 2026".

Summit uses Phoenix Infrastructure, LLC ('Csquare'), Coloware, Digital Realty Trust, Inc. ('Digital Realty'), Equinix, Inc. ('Equinix'), Flexential Corp. ('Flexential'), H5 Data Centers, Sabey Data Center Properties, LLC ('SDC'), Telehouse International Corporation of Europe Ltd ('Telehouse'), and Web Werks India Private Limited ('Web Werks') to provide colocation services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Summit, to achieve Summit's service commitments and system requirements based on the applicable trust services criteria. The description presents Summit's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Summit's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Summit's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Summit's controls.

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 period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Summit's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Summit's controls operated effectively throughout that period.

A handwritten signature in blue ink that reads "Randy Raitz". The signature is written in a cursive, flowing style.

Randy Raitz
VP, IT & CISO
Summit Hosting LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To Summit Hosting LLC:

Scope

We have examined Summit's accompanying assertion titled "Assertion of Summit Hosting LLC Management" (assertion) that the controls within Summit's IT Services System were effective throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Summit's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*.

Summit uses Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse, and Web Werks to provide colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Summit, to achieve Summit's service commitments and system requirements based on the applicable trust services criteria. The description presents Summit's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Summit's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Summit, to achieve Summit's service commitments and system requirements based on the applicable trust services criteria. The description presents Summit's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Summit's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Summit 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 Summit's service commitments and system requirements were achieved. Summit has also provided the accompanying assertion (Summit assertion) about the effectiveness of controls within the system. When preparing its assertion, Summit 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 management's assertion that 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 AICPA. 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 description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

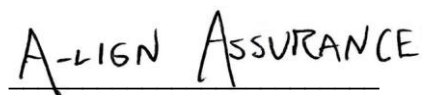
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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, management's assertion that the controls within Summit's IT Services System were suitably designed and operating effectively throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Summit's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Summit's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Summit's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.


Tampa, Florida
July 17, 2026

SECTION 3

SUMMIT HOSTING LLC'S DESCRIPTION OF ITS IT SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2025 TO JUNE 30, 2026

OVERVIEW OF OPERATIONS

Company Background

Summit is established as a trusted advisor for its clients. The Summit team humanizes technology. Summit partners with clients while learning and collaborating to develop tailored solutions for client needs. Summit designs, builds, operates, secures, and scales unique technology solutions with the singular purpose to deftly deliver on the promise of technology for its clients and their customers.

Summit provides global network and data center services, cloud consulting, managed cloud infrastructure, and managed information technology (IT) services to startups, enterprises, and Fortune 500 companies across North America, Europe, Australia, and Asia. Summit provides services 24 hours a day, 365 days a year (366 on leap years) with nominal downtime.

Summit is a managed IT solutions provider specializing in custom technology infrastructure solutions. From data centers strategically located worldwide, Summit serves a diverse roster of companies including content delivery companies, web hosting, and application service providers in addition to companies in more traditional industries including, but not limited to, financial services, healthcare, consulting and professional services, and high technology. Summit provides managed data center, network, and cloud services to its customers globally.

Description of Services Provided

Infrastructure Colocation

Summit's Infrastructure Colocation services provide organizations with premium data center space, power, cooling, network connectivity, and security services necessary for the operation of IT infrastructure requiring maximum uptime and availability. This service is provided within Summit-operated data centers and can be used with a variety of complementary services, including remote hands, enhanced security, advanced monitoring, infrastructure migrations, managed connectivity to customer-operated on-premise infrastructure, and managed links to third-party cloud platforms including, but not limited to, AWS or Azure.

Summit chooses facilities that are essential to geographic markets worldwide, enabling Summit to provide reliable service to any geographic market. Summit's data centers are strategically selected by considering facility design, engineering, and redundancy. In order to provide network services, Summit considers access to diverse carriers and metro fiber routing to provide the most resilient network access.

Summit has developed several services that focus on enhancing its customers' operations, including scalable bandwidth options, managed network equipment including firewalls, remote hands, as well as reliability products including monitoring, data storage, backup, offsite archiving, out-of-band access, and disaster recovery. Trained staff are available continuously to install, configure, and troubleshoot equipment and services.

Internet Protocol (IP) Transit Service

Summit offers Internet connectivity to, from, and between its data centers which are designed for low latency, rapid bursting, and carrier diversity. The IP network is built with physical device and path redundancy to ensure maximum service availability while ensuring reliability and redundancy required by customers. In markets where IP Transit is available, core network equipment is deployed in a redundant fashion and connected to multiple, diverse 10-gigabit connections to carriers, insuring failover of IP traffic if any carrier loses connectivity.

Metro Ethernet

Summit's Metro Ethernet service offers customers fixed-rate Ethernet capacity between facilities in the same market (i.e., Chicago and its suburbs). This makes it easy for customers to reach carriers that may be in a different location than the customer's equipment, or implementation of backup/disaster recovery strategies. Metro Ethernet is available in 1 Gigabit, 10 Gigabit, and 100 Gigabit Ethernet speeds.

Multi-Protocol Label Switching (MPLS) Virtual Private Network (VPN)

Summit's global backbone runs MPLS, which allows the provisioning of private point-to-point connections between two or more locations on the Summit network, sold under either fixed or variable capacity. This means that extra capacity is available on demand, allowing customers to burst beyond their committed bandwidth levels, instead of dropping the excess data. Data transport is available at speeds from 1 Megabit to 100 Gigabits and beyond.

Services Overview

Professional Services

Remote Hands

Customers who contract for colocation services in one of Summit's data centers have the opportunity to utilize trained data center staff from Summit to diagnose, troubleshoot, and repair their equipment through Summit's Remote Hands service. Examples of tasks that can be performed include operating system installation, cabling, cabinet installation, inventory reporting, and more. Customers can contract for blocks of hours to be used on a monthly basis or request emergency work at hourly rates.

Network Engineers and System Administrators

Summit's network is monitored 24x7x365 by Network Engineers and System Administrators with the expertise available to maintain a competitive advantage and exemplary customer service. The engineers and administrators also monitor and support the various managed services described above.

Data Erasure, Destruction, and Equipment Disposal

Summit offers its customers several methods to securely erase or destroy data, as well as recycle obsolete equipment. Upon request, a Certificate of Erasure or Certificate of Destruction will be issued to a customer upon completion of the service.

Data Center Migration

Summit's Chicago-based team has developed a reliable methodology and process for migrating customer equipment into Summit's facilities. This includes project planning, timeline development, auditing and documentation, layout and cabling design, as well as the physical moving processes and required post-migration validation.

Cloud Migration

Summit has developed a reliable methodology and process for migrating customer environments to private and public cloud platforms, including hybrid and multi-cloud configurations. This includes project planning, timeline development, auditing and documentation, as well as the application and data moving processes, security moving processes, and required post-migration validation.

Cloud / DevOps Consulting

Summit has developed reliable methodologies and processes for helping customers adopt DevOps best practices and implement them throughout their organizations. This includes project planning, timeline development, training and documentation, as well as the implementation and management of new technology and businesses processes throughout customer organizations.

Cloud-Native Software Development

Summit provides comprehensive cloud-compatible and cloud-native software development services. Cloud-native software development projects can range from refactoring - customizing, adapting, and evolving - applications and application programming interfaces (APIs) to address business challenges and meet current and future cloud standards to creating fully custom, net-new applications. Summit also provides ongoing application management and support as required by the customer.

Managed Services

Summit offers its customers a full catalog of managed services which depend on Summit's knowledge and experience to implement complex technical solutions. Summit's engineers develop and follow detailed workflows to monitor systems, isolate problems, troubleshoot hardware and software, contain issues, and restore services, as well as provide updates and information to the customers as specified. Most managed services are offered with standard- or high-availability configuration options.

Summit provides clients with access to a Customer Portal where they can view key aspects of their products/services including a listing of assets (racks, servers, switch ports), the usage of their power and network services, a repository of sales orders and legal documents, as well as network security and monitoring tools. Summit's staff of developers release new features and updates to the Customer Portal.

Firewalls, Load Balancers, Switches and Routers, Distributed Denial of Service (DDoS) Mitigation, and VPN Appliance

Summit's suite of managed network device services is designed to maximize uptime and provide continuous protection against malicious activity. A firewall ensures that hackers and Internet worms are stopped before they reach critical servers. A Load Balancer distributes workloads across multiple computing resources and network paths to optimize resource utilization and increase application availability. Switches and routers serve as the core Layer 2 and Layer 3 infrastructure for a customer and the gateway to Summit's networks and public Internet. DDoS mitigation services provide detection and mitigation of volumetric network attacks from external or internal networks. VPN services ensure secure point-to-point access to customer resources using standards-based encryption and hardware.

Summit's staff is responsible for the configuration and maintenance of the devices included in the managed service. Security analysts work closely with customer IT teams to ensure that the right security posture is executed, and business functions remain fluid while threats are discovered and controlled. Devices managed by Summit are continually monitored and adjusted to account for changes in technology requirements and business needs.

Managed Network Attached Storage (NAS) and Storage Area Network (SAN) Solutions

Summit single- and multi-tenant storage systems are continuously monitored and secured in its facilities. Servers and autonomous networks are connected to the storage fabric via defined network segments to ensure data security and service reliability. Traffic to and from systems is secure and never exposed to other customers. Data is stored according to both Customer's individual security needs and applicable compliance requirements.

Managed Backup

Summit provides customers with fully managed and internally architected hardware and software solutions to backup, replicate, and (optionally) restore copies of protected data. Summit leverages industry-leading solutions to backup customer data, physical machines, and virtual hosts. Tools including Unitrends, Veeam, Zerto, and replication tools are built into various storage and virtualization platforms. Summit is also a Veeam Cloud Connect provider.

Managed Cloud Storage

Summit provides a full spectrum of managed cloud storage services. Summit's Cloud Storage offerings are flexible, scalable, and secure, allowing customers to dynamically scale storage in response to changing business needs. Managed Cloud Storage Services are delivered from Summit's global data centers as well as third-party public cloud platforms including AWS, giving Customers the option to deploy resources in the most appropriate locations. Managed Cloud Storage is architected for support of applications and data with performance requirements. Summit currently offers four types of Managed Cloud Storage Services: Multi-tenant Storage, Dedicated Storage, Object Storage, and AWS Storage.

Monitoring Services

Summit can monitor nearly any service on any platform (inside or external to Summit's data centers) to ensure alerting on functionality of systems and network devices. The monitoring platform is built upon industry-standard software to provide accurate and instantaneous notifications to the Network Operations Center (NOC) staff, who manage the notifications and alerts. Summit engineers have developed probes and monitors for dozens of customer-specific applications and systems to ensure constant uptime. Engineers also monitor systems proactively to avoid service-impacting downtime and verify system compliance from Summit's data centers.

Dedicated Servers

Dedicated Servers are for customers who prefer to have Summit provide, maintain, and operate their server infrastructure. Each server's standard configuration already includes high-performance processors and memory, and servers can be configured with high-availability storage. Summit maintains an extensive inventory of spare parts to facilitate quick upgrades and maintenance.

Summit's Dedicated Server service goes beyond the components inside the server chassis and includes Summit's trained Data Center Operations group, available 24x7x365 to monitor and assist customers with services. Summit's dedicated servers are available in most Company colocation facilities and are connected to Summit's IP network.

Cloud Assessments

Summit follows a structured process of data collection and analysis via a series of interviews with key business stakeholders, IT infrastructure, and application teams to complete a Cloud Assessment.

The outcome of these meetings is combined with the output from automated assessment tools to establish a comprehensive data set that includes business rules, hardware inventories, application inventories, application snapshots, functions, and dependencies.

This comprehensive data set is then synthesized and coupled with Summit's experience in engineering Managed Cloud Solutions to create the project deliverable - a Cloud Roadmap.

The outcome of the Cloud Assessment delivers:

- A detailed understanding of the specific costs of each cloud platform and the application and data migration processes.
- A clear identification of the gaps between current infrastructure and application architecture and next- generation cloud architecture.
- Formal recommendations of the right cloud hosting options (public cloud, private cloud) for each application in question.
- A clear identification of the impact to existing development and deployment modes.
- An understanding of the impacts to existing licensing.
- Identify appropriate tools for server / application / data / physical system migrations.
- A formal plan to achieve each customer's stated objectives.

Managed Public and Private Clouds

While cloud computing is at the forefront of IT, individual customer requirements dictate a flexible approach to Summit's cloud offerings. Integrating the colocation space and power, server and storage infrastructure, network connectivity, hypervisor and control plane, Summit is an infrastructure provider with a focus on supporting large-scale enterprise and content provider workloads.

Summit's high-performance managed clouds provide on-demand access to the infrastructure, applications, and data needed to satisfy financial, operational, and IT objectives. Summit manages installation and maintenance and is backed by Summit's comprehensive Service Level Agreements (SLAs).

Special Features include:

- Continuous onsite technical support.
- Global footprint of high-quality, reliable data centers.
- Simple demonstrations of usability and function.
- Flexible storage interface with SAN, NAS, content storage, and translators.
- Petascale storage, load balancing, web application firewall, firewall, relational database, and service monitoring are available.
- Support for live virtual machine ware (VMware) migrations.
- Seamless integration with VMware, Xen, kernel-based virtual machine (KVM), and more.
- Delivers content and runs databases at 10+ gigabits per second performance.

Disaster Recovery as a Service (DRaaS)

Summit's DRaaS is a combination of automated protection of virtual machines, a managed service to coordinate the ongoing real-time replication of data between two sites, managed failover testing on a regular basis, and managed failover and failback in the event of a declared disaster. Summit's DRaaS provides the ability to failover a virtualized environment to a Summit data center in response to a declared disaster. Upon declaration of a Disaster Event, Summit and the Customer will perform the pre-defined set of activities set forth in a mutually agreed-upon Runbook. DRaaS includes the option to run additional tests upon request.

Special Features:

- Based on reputable hardware and software.
- Highly available, resilient, and secure design.
- Automated protection of virtual machines in near real-time.
- Managed failover and failback of virtual machines (VMs).
- Collaborative planning and assessment of Customer needs.
- Based on Customer-defined recovery point objective (RPO), recovery time objective (RTO), and business needs.
- Includes synchronization of physical devices used with the Service.
- Service documented in Summit-maintained Runbook.
- Initial and annual full failover and failback test, with option for additional tests.
- Complete infrastructure configuration and administration by Summit.
- 24x7 continuous monitoring, alerting, and support of the infrastructure.
- Secure Customer Portal for documentation and service requests.

Principal Service Commitments and System Requirements

Summit designs its processes and procedures related to its IT Services System to meet its objectives for its services. Those objectives are based on the service commitments that Summit makes to user entities, the laws and regulations that govern the provision of hosting, managed services, and cloud operations services, and the financial, operational, and compliance requirements that Summit has established for the services. The services of Summit are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Summit operates.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following listed below:

- Security principles within the fundamental designs of the IT Services System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

Summit establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Summit's system policies and procedures, system design documentation, and contracts with customers. 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. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the IT Services System.

Components of the System

Infrastructure

Summit invests heavily in enabling data center network infrastructure. Utilizing redundant routers and extensive failover topology + programming, the network is designed to prevent any single point of failure from causing an impact to service. Clients are encouraged to utilize two or more diverse connections to the Summit network to ensure maximum uptime.

Primary infrastructure used to provide Summit's IT Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Dell EMC SuperMicro	Physical Servers	Compute services used to deliver virtual and dedicated infrastructure
Pure Storage Nimble Hewlett Packard Enterprise (HPE)	Storage Appliance	Data storage for virtual infrastructure and other enterprise needs
Mellanox Switches	Network Equipment	Enables low-latency, high-throughput networking for inter-server communication and storage access within data centers
Juniper Switches and Routers	Network Equipment	Manage, secure, and route high-speed data traffic within the infrastructure
Cisco Switches	Network Equipment	Manage, secure, and route high-speed data traffic within the infrastructure
Palo Alto Firewalls	Network Equipment	Secure and manage data traffic, provide firewall protections
Fortigate Firewalls	Network Equipment	Secure and manage data traffic, provide firewall protections

Software

Enterprise monitoring tools and custom scripts monitor critical system events. Upon the occurrence of an event, an alert is created in Summit's ticketing system and immediately escalated to administrators for triage and resolution. Summit's ticketing system is a web-based application used for issue tracking and requests for service and is the primary means of communication. Summit utilizes enterprise-level antivirus for virus/vulnerability scanning and VPN with multi-factor authentication (MFA) for remote employee access to the System.

Primary software used to provide Summit's IT Services System includes the following:

Primary Software		
Software	Operating System	Purpose
VMware vSphere	Elastic Sky x (ESXi)	Support and deliver virtual infrastructure
Veeam	Microsoft Windows	Managed backup and restoration capabilities
Fire Hydrant	Software as a Service (SaaS) Application	Incident management

Primary Software		
Software	Operating System	Purpose
Github	SaaS Application	Continuous integration and continuous deployment (CI/CD) Pipeline Management, Code Repository
LogicMonitor	SaaS / On-prem Hybrid	Infrastructure Monitoring and Alerting
Global Protect	Multiple	Remote access VPN client supported by Palo Alto Firewalls
Microsoft Defender	Multiple	Security information and event management (SIEM) system, extended detection and Response (XDR) solutions used to protect, detect and respond to advanced cyberattacks
Remote Desktop Gateway	Windows Server	To act as a gateway that enables authorized users to connect to their designated desktops. It uses secure remote desktop protocol (RDP) over hypertext transfer protocol secure (HTTPS) to establish a safe and encrypted connection
TruGrid SecureRDP	Windows Server	TruGrid allows users and staff to access their designated servers from anywhere, leveraging MFA and end-to-end encryption
Microsoft Entra	SaaS	Provides centralized identity and access management, enabling secure authentication, single sign-on (SSO), conditional access policies, and MFA across integrated services and applications
SentinelOne	SaaS	Endpoint detection and response (EDR) software that uses AI-based threat prevention, detection, and automated remediation to protect against malware, ransomware, and other threats
Akamai Guardicore	SaaS	Micro segmentation and breach detection platform that provides visibility, policy enforcement, and threat detection across hybrid environments. Helps isolate workloads, limit lateral movement, and ensure compliance with data protection regulations
ZenDesk	SaaS	Provides a centralized platform for managing customer support and internal service requests, enabling ticket tracking, audit logging, workflow automation, and secure communication between teams and clients

People

Summit has a team of more than 250 individuals across North America and other international locations that are responsible for the overall design, operation, and support of Summit's products and services. This team consists of the following departments:

- Finance
- Sales
- Software Development
- Managed Services

- IT
- Security and Compliance
- Human Resources (HR) and Administration
- Data Center Operations
- Customer and Technical Support
- Systems Administration
- Network Engineering
- Cloud Services

Candidates at Summit undergo a background check prior to employment. Additionally, credit history is considered in positions of financial oversight, or where access to Company or customer data and/or assets is required by the employee.

Employees abide by Summit's security and confidentiality requirements outlined in its employee handbook, and employees acknowledge the code of conduct annually. Any violation of policy will result in immediate action up to, and including, termination and legal action. Employees are also trained on proper computer usage, Internet usage, e-mail-based threats, social media interaction, and proper client data handling.

Data

Access to data is limited to authorized personnel in accordance with Summit's policies on system security administration. The Systems Administration and Network Engineering teams are responsible for the overall availability of data, including system backups, monitoring of data processes, file transmissions, and identifying and resolving system problems.

Summit utilizes multiple network and security functions, including IPsec VPN, antivirus/malware/spyware solutions, and security information and event management tools.

Summit's networks are protected by enterprise-class firewalls with special custom routing for services and appropriate enterprise-class virus protection. Summit endpoints are password-protected with appropriately assigned user rights and MFA.

Customer Owned Data

Customer Owned Data refers to information owned by Summit's clients and entrusted to the systems for secure storage and utilization. Summit maintains an unwavering commitment to the protection of Customer Owned Data, safeguarding it against unauthorized access, accidental alterations, or malicious deletions. The stringent Data Retention and Confidentiality Policies play a pivotal role in ensuring the security and integrity of this data.

Operational Data

Operational Data comprises a diverse range of information, configurations, and intellectual property utilized by Summit's Technical Operations. This data is essential for delivering seamless services to clients and ensuring the uninterrupted functioning of business operations at levels. It encompasses various domains, including Data Center Operations and Infrastructure, Customer Logon Systems and Environments, as well as broader Business Operations, such as HR, Payroll, and Benefits management.

Summit is committed to the responsible management and protection of both Customer Owned Data and Operational Data, adhering to the highest standards of security and confidentiality.

Processes, Policies and Procedures

Procedures are used to achieve the data security and confidentiality objectives of Summit and its clients in accordance with defined policies and governmental regulations. Summit has highly experienced IT, network, and systems teams that are fully qualified to manage, design, implement, configure, and modify deployed infrastructure consistent with Summit's system security and confidentiality policies.

Complex network passwords and password expiration procedures are in place to restrict logical access to Summit and client systems that include the identification and authentication of users. New user requests or changes to existing users undergo a formal approval process and are tracked in Summit's systems. Access to offline storage is managed internally and restricted to authorized Summit personnel. Summit's technical teams maintain strict control over access to system configurations, user functionality, master passwords, and security devices.

In addition to strict system-access granting, Summit employs measures to prevent unauthorized access to the system. When accessing Summit systems remotely, a secure VPN connection through the network firewall is required, utilizing MFA. Confidential data and user authentication information is encrypted when transmitted over the Internet. Intrusion detection systems (IDS) are in place, as well as antivirus software, through the use of a SIEM tool which are installed on systems to prevent infection by computer viruses and other unauthorized software/malware. Should there be any access violations, Summit has developed an incident response plan that addresses incidents and noncompliance.

Procedures designed to support system maintenance have been established to ensure any changes to the system are consistent with Summit's security and confidentiality policies and that they have been authorized, tested, and documented whether they are planned or unplanned.

Physical Security

The in-scope system and supporting infrastructure is hosted by Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse, and Web Werks. As such, Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse, and Web Werks are responsible for the physical security and environmental controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse, and Web Werks.

Logical Access

Access to resources and data is granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests. The IT Manager is the security administrator and is responsible for ensuring adherence to the security policy that addresses logical access control procedures.

Unique user identifiers (UUIDs) and passwords are assigned to each user. Summit's security policy establishes password rules, which require a minimum of eight characters with password complexity requirements. Passwords are systematically required to be changed in accordance with AD policy. The system administrator sets the user's initial password. The user is required to change the password at first login.

IT or data owners remove individual access capabilities within a reasonable amount of time upon notification of termination of employment, change of responsibilities, or termination of a contract with a client that uses the system.

Employees accessing the system from outside the Summit network are required to use MFA. Employees are issued software tokens upon employment, and which are revoked upon termination. Vendor personnel are not permitted to access the system from outside the Summit network.

Upon hire, employees are assigned to a position in the HR management system. The HR team creates a creates an onboarding ticket specifying the start date and the employee's role, which dictates the access that will be provisioned by the internal IT Team. Access rules have been pre-defined based on the defined roles.

On a quarterly basis, access reviews of account holders are conducted by a working group composed of security, IT, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed access reviews are evaluated and approved by the Chief Information Security Officer (CISO). As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR team generates a ticket for each employee or contractor termination event specifying the date and time access should be terminated. The tickets are assigned to the internal IT team to terminate employee access in a timely manner. On an annual basis, HR runs a list of active employees. The internal IT team uses this list to suspend user identification (IDs) and delete access roles from IDs belonging to terminated employees or users not on the HR list.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Production data is backed up and replicated daily, and Summit retains 15 days' worth of recovery points, unless specified by a specific client SLA or procedure. Backup restoration tests are performed quarterly to ensure backup restoration activities operate effectively. Backup services are provided as part of a Managed Service and are required to be subscribed to or included in a product's SLA if they are to provide client data backup services.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Summit monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs. Summit evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Infrastructure capacity monitoring includes but is not limited to managing data center space, power, and cooling to ensure optimal performance and reliability. The software oversees disk storage capacity and network bandwidth to support efficient data access and system scalability.

Summit takes a proactive approach to patch management. Summit administrators regularly monitor various web sites, message boards, and mailing lists where advanced notification of bug and related patches are often disclosed prior to a public announcement by the vendor. This allows Summit to plan ahead for upcoming patches.

Summit administrators consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability being addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the intrusion prevention system (IPS), or an aspect of the hardening process. In these cases, patches may be deferred until they are included in a future service pack.

Change Control

Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

Zendesk, the ticketing system and Github are utilized to document the change control procedures for changes in the application and implementation of new changes. Quality Assurance Testing (QAT) and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the applicable tracking system.

GitHub, the version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. Github serves as the version control system for automation platforms / frameworks as well.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Summit. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a weekly basis in accordance with Summit policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Summit. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Summit system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based MFA system.

Boundaries of the System

The scope of this report includes the IT Services System performed in the Alpharetta, Georgia; Denver, Colorado; and remote locations.

Summit's IT Services System is hosted in the infrastructure colocation sites in:

- Csquare ORD1, Chicago, Illinois
- Csquare IAD1-A, Sterling, Virginia
- Coloware, Toronto, Canada
- Digital Realty CH1, Elk Grove Village, Illinois
- Digital Realty CHI1, Chicago, Illinois
- Digital Realty IAD1, Ashburn, Virginia
- Digital Realty DFW1, Dallas, Texas
- Digital Realty SJC1, Santa Clara, California
- Digital Realty FRA11/FRA16, Frankfurt, Germany
- Digital Realty, JNB1, Johannesburg, South Africa
- Equinix AM1/AM6, Amsterdam, Netherlands
- Equinix CH1/CH2/CH3/CH4, Chicago, Illinois
- Equinix DC2/DC3/DC4/DC6, Ashburn, Virginia
- Equinix MI1, Miami, Florida
- Equinix ME2, Melbourne, Australia
- Equinix SP4, Sao Paulo, Brazil
- Equinix SV1/SV3/SV4/SV5, San Jose, California
- Equinix SY1/SY2/SY3/SY4, Sydney, Australia
- Equinix TY1, Tokyo, Japan
- Equinix DA6, Dallas, Texas
- Equinix FR2/FR7, Frankfurt, Germany
- Flexential, Atlanta, Georgia
- H5 Data Centers, Denver, Colorado
- SDC, Seattle, Washington
- Telehouse London-North, London, United Kingdom
- Web Werks, BOM1, Mumbai, India

This report does not include the colocation services provided by Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse or Web Werks for the above facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the last review.

Criteria Not Applicable to the System

All Common/Security criteria were applicable to the Summit IT Services System.

Subservice Organizations

This report does not include the colocation services provided by Csquare, Coloware, Digital Realty, Equinix, Flexential, H5 Data Centers, SDC, Telehouse, and Web Werks. See 'Boundaries of the System' section above for the colocation sites at the various facilities.

Subservice Description of Services

Each subservice organization facility is fully equipped with redundant uninterruptable power supply (UPS), backup generators, and cooling systems. Only facilities with the highest standards, including proactive maintenance on critical systems, are chosen for Summit's global data center footprint.

Infrastructure Colocation Key Details include:

- High security facilities with continuously staffed security teams.
- Redundant backup power and heating, ventilation, and air conditioning (HVAC) infrastructure.
- Environmental and fire protection systems.
- Full network redundancy with multiple carriers and backbone diversity.
- Large inventory of spare parts including drives, power supplies, memory, fiber, cables, network optics, processors, and fans.
- While the standard offering is individual locking cabinets, private cages, and smaller cabinet compartments are available in certain markets.

Complementary Subservice Organization Controls

Summit's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to Summit's services to be solely achieved by Summit control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Summit.

The following subservice organization controls should be implemented by Csquare and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Csquare		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Site authorizers are utilized to approve permanent access to the data centers.
		Security access controls (i.e., physical barriers and doors, card controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities.
		Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.
		Data center badge access requests for Company employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.
		Data center access for Company personnel is revoked as a component of the employee termination process.
		Temporary access to the data centers for Company contractors must be pre-approved by a work order or ticket. Temporary access to data centers for customers requires prior authorization by the authorized customer representative.

Subservice Organization - Csquare		
Category	Criteria	Control
		Customer-maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.
		Visitor logs are maintained for at least 90 days to document visitor activity at the data centers.
		Visitors are required to be escorted by an authorized Company employee or authorized customer representative at all times while in the data centers.
		An inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by location, is performed at least once per day to account for all badges and metal keys.
		Badge access reviews are performed annually to help ensure that access to the data center facilities is restricted to authorized personnel.
	CC6.4, CC7.2	CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.
		Data center security personnel and the PSCC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.
		The badge access system is configured to monitor for security events within the data center (forced entry, door held open, etc.) and notify security personnel when predefined thresholds are exceeded on monitored devices.

The following subservice organization controls should be implemented by Coloware and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Coloware		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Access throughout the data center is controlled through the use of key card readers/badges.
		Visitors to the data center facility are required to register in a visitor log prior to accessing the facilities. Visitors must be escorted by an authorized badge holder while on the premises.
		Visitor logs are reviewed by a Coloware Operations Technician to determine that the logs were filled out completely.
		Coloware tracks data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.
		Changes to data center facilities and systems that may affect system availability and security are communicated to employees and customers via e-mail.

Subservice Organization - Coloware		
Category	Criteria	Control
	CC6.4, CC7.2	Badge access lists are reviewed by a Coloware Operations Technician to determine that access to the data center is limited to authorized employee and customer personnel.
		Data centers are equipped with video surveillance cameras located throughout the premises to monitor and record activity and footage is retained for a minimum of 90 days.

The following subservice organization controls should be implemented by Digital Realty and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Digital Realty		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access controls are in place to restrict access to and within the data center facilities.
		Physical access requests are documented and require the approval of the relevant access authorizer.
		A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed.
		A termination notification ticket is completed by HR, and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification.
		Escorted visitors are required to surrender their badges at the end of the day.
	CC6.4, CC7.2	Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers.
		Digital surveillance systems are configured to retain video footage for the in-scope data center facilities for a minimum of 90 days or maximum allowed by local legislation.

The following subservice organization controls should be implemented by Equinix and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Equinix		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Procedures exist and are followed to establish and make changes to physical access privileges for customers.
		Procedures exist and are followed to establish and make changes to IBX physical access privileges for Equinix employees who have a need to access an IBX.
		For offsite employees, customers, vendors, and contractors, onsite security or Equinix personnel review valid government issued photo identification prior to allowing access to IBX data centers.
		Visitor access procedures are in place requiring: • Visitor sign into a log upon entry to the IBX data center facilities • Visitors are to be escorted by an authorized employee when accessing the IBX data center facilities
		Dual control biometric, four-digit personal identification numbers and / or proxy card readers are in place to help ensure that only authorized individuals have the ability to access the IBX data center, warehouse area, and storage cages. This control shall be applied as and where applicable.
		Biometric hand scan and / or proxy card access to the IBX data centers is electronically logged and maintained as per data privacy laws. Exceptions or attempts of unauthorized access are tracked and escalated.
		Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.
		CCTV surveillance cameras are in place to monitor and record activity at the entrances to and throughout the IBX data center facilities. Surveillance camera logs are recorded and maintained minimum of 90days unless specified otherwise per local country law/regulation for IBX data center facilities.
		Ingress mantraps are in place and administered to restrict access to IBX data center facilities to only authorized individuals. Else, there needs to be continuous monitoring of IBX access doors leading to the exterior.
		Each customer has defined space within the IBX data center that is physically secured within a locked cage and / or cabinet.
		The data center floor does not have windows leading to the exterior of the building, where applicable. In cases due to the existing infrastructure having windows and entry points leading to the exterior, then they need to be locked from the inside or access controlled.
		Physical access reviews are documented and approved by information security personnel at least annually for IBX data centers.

Subservice Organization - Equinix		
Category	Criteria	Control
	CC6.4, CC7.2	IBX facilities are monitored 24x7 by facilities engineers. Equinix has staff in place either onsite or on call 24x7 who are alerted by the BMS for system exceptions.

The following subservice organization controls should be implemented by Flexential and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Flexential		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: - Flexential badge to enter the building - Badge and PIN code, or a badge and biometric fingerprint scan to enter the data centers
		Visitors are required to sign-in with onsite security personnel prior to entering the data centers.
		Data center visitors are required to be accompanied and supervised by an authorized Flexential employee or client escort.
		Visitors are required to wear a visitor badge while visiting the data centers.
		Client equipment is maintained in lockable cages or racks within the data centers.
		There are no exterior facing windows in the walls of the areas where client production servers are located.
		Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.
		Management reviews badge access of terminated employees on a quarterly basis.
		Badge access privileges of terminated employees are revoked as a component of the employee termination process.
	CC6.4, CC7.2	A digital surveillance system is in place to record activity in the data centers.
		Technical assistance center personnel are staffed at the data center facilities 24x7 to monitor facility access and log visitors.

The following subservice organization controls should be implemented by H5 Data Centers and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - H5 Data Centers		
Category	Criteria	Control
Common Criteria / Security	CC6.4; CC7.2	Policies and procedures are in place to guide personnel in physical security activities.
		Logical and physical access privileges are reviewed on a semi-annual basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.
		The main data center building entry point requires badge access to prevent unauthorized access. Visitors to the data centers are required to sign in and be escorted by an authorized data center employee.
		Visitors are required to provide photo identification, sign an electronic visitor log, and complete a nondisclosure agreement prior to entering the data center facilities.
		Management assigns badge access privileges to users utilizing pre-defined access zones to help ensure that access privileges are consistently assigned based on job responsibilities.
		A badge access or dual-authentication (biometric) access system exists to control access movement into and throughout the facilities.
		Privileged access to the badge access system is restricted to authorized personnel.
		Access to the data center is restricted through a mantrap system where available. In facilities where a mantrap is not present, camera monitoring is implemented to oversee access attempts. Surveillance footage is retained for at least 90 days to detect and respond to unauthorized access. Badge based authentication is required for entry, and access logs are maintained for audit purposes.
		Physical access to systems is revoked as a component of the termination process.
		A manned reception desk is in place to monitor and control access to the entrance of the office facilities during standard business hours.
		On-site security personnel monitor the physical security of the data center facilities 24 hours a day.
		Visitors to the data center facilities are provided with a visitor badge after photo identification verification has been completed and are required to be escorted and supervised by a data center employee or authorized client personnel.
		User access to the badge access system is reviewed on a semi-annual basis.
	CC6.4, CC7.2	The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.
		A video surveillance system is in place with footage retained for 90 days.

The following subservice organization controls should be implemented by SDC and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - SDC		
Category	Criteria	Control
Common Criteria / Security	CC6.4; CC7.2	A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.
		A badge access system controls access to and within the office facilities.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.
		The badge access system logs successful and failed access attempts. The logs can be pulled for review if necessary.
		Privileged access to the badge access system was restricted to persons holding the authorized positions.
		Access to the server is restricted to badge access cards assigned to appropriate personnel.
		A video surveillance system is in place with footage retained for 30 days or until storage capacity is reached.
		Visitors to the facility and server room are required to be escorted by an authorized employee.
		Visitors to the facility are required to sign a visitor log prior upon arrival.
		Physical access privileges to the corporate office facility are revoked as a component of the termination process.
		User access to the badge access system is reviewed on quarterly basis.
		CCTV cameras monitor physical access to the entity's facilities and visitor access to the facility and server room require the visitor to sign a visitor log prior upon arrival.

The following subservice organization controls should be implemented by Telehouse and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Telehouse		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Policies and procedures are in place to guide personnel in physical security activities.
		Physical access to systems is approved and granted to an employee as a component of the hiring process.
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.
		A badge access system controls access to and within the office facility.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.
		Privileged access to the badge access system is restricted to authorized personnel.
		Access to the server room / data center is restricted to authorized personnel.
		Visitors to the office facility and server room / data center are required to be escorted by an authorized employee.
		Physical access is reviewed on at least an annual basis.
	CC6.4, CC7.2	The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.
		A video surveillance system is in place with footage retained for a minimum of 90 days.
		CCTV cameras monitor physical access to the entity's office facilities and visitor access to the office facilities and server room / data center require the visitor to sign a visitor log prior upon arrival.

The following subservice organization controls should be implemented by Web Werks and included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - Web Werks		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Formalized policy and procedure exist for managing physical access to Web Werks facilities and Data Centers. These policy and procedure are approved by the Senior Management of Web Werks on an annual basis.
		Access to Data Centers is restricted to authorized personnel from Administration team, DCOps team and Network team.
		Employees and visitors undergo security scans using metal detectors and X-Ray bag scanner machines before being permitted inside the facilities.
		Security guards or receptionists are responsible to help ensure that the details of the visitors such as name of visitor, organization name, contact details, contact person, entry and exit time, details of assets being carried by the visitor are recorded within the Visitor Management System (VMS) maintained at the reception for permitting entry to Web Werks facilities. Visitors are also required to present a government issued or company issued photo identification card.
		Web Werks has different color-coded access belt defined for employees and visitors. Visitors are escorted by Web Werks representative inside the Web Werks facilities and Data Center.
		Proximity card-based access control systems are installed at entry and exit points to restrict unauthorized entry into Web Werks facilities.
		Access to Data Center Server Hall is controlled by a combination of proximity card-based access system and biometric access.
		Web Werks has created mantraps to restrict access of the Data Center to authorized personnel.
		On the day of joining, new hire (employee or contractor) or team member of the new hire sends an e-mail request with details such as job profile and level of access to the new hire's reporting manager and facility manager. Once the request is approved by the new hire's reporting manager over e-mail, the Administration team grants access to approved areas to the new hire.
		On the last working day of a resigned employee, employee returns the physical access card to the Administration team. Administration team deactivates employee's physical access to Web Werks facilities and Data Centers and provides sign off and on the 'Exit Clearance' form.
		On the last working day of a contractor, contractor personnel return the physical access card to the Administration team. Administration team deactivates the employee's physical access to Web Werks facilities and Data Centers.

Subservice Organization - Web Werks		
Category	Criteria	Control
		On a monthly basis, Administration team reconciles the list of leavers (employees and contractors) with the list of users (employees and contractors) having active physical access to Web Werks facilities. Discrepancies, if any, are tracked to closure by the Administration team. The access reconciliation report is reviewed and approved by Head Administration team.
		On a monthly basis, Administration team extracts the list of personnel having access to the Data Centers and shares it with the Network team and DCOps team. The Network team and DCOps team review the appropriateness of the physical access and communicate the discrepancies, if any, to the Administration team. Administration team takes corrective action and tracks the discrepancies to closure. The access review report is reviewed and approved the Head - Network team and General Manager - DCOps team.
	CC6.4, CC7.2	Physical Security at Web Werks begins from the perimeter of Web Werks facilities. Security guards or receptionists are stationed 24/7 at entry - exit points and other strategic locations to monitor the physical access to Web Werks facilities and Data Centers.
		Closed Circuit Television (CCTV) surveillance equipment is used by the Administration team to monitor the entry and exit points at Web Werks facilities and strategic locations (entry / exit points and server aisles) within the Data Centers to monitor and record activities. Administration team monitors the CCTV footage on a real-time basis. CCTV logs are retained for a minimum of 90 days.

Summit management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, Summit performs monitoring of the subservice organizations controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations.
- Making regular site visits to vendor and subservice organizations' facilities.
- Reviewing attestation reports over services provided by vendors and subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

Summit's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Summit's services to be solely achieved by Summit control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Summit's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Summit.
2. User entities are responsible for notifying Summit of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Summit services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Summit services.
6. User entities are responsible for providing Summit with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for determining if a backup needs to be restored.
8. User entities are responsible for immediately notifying Summit of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.