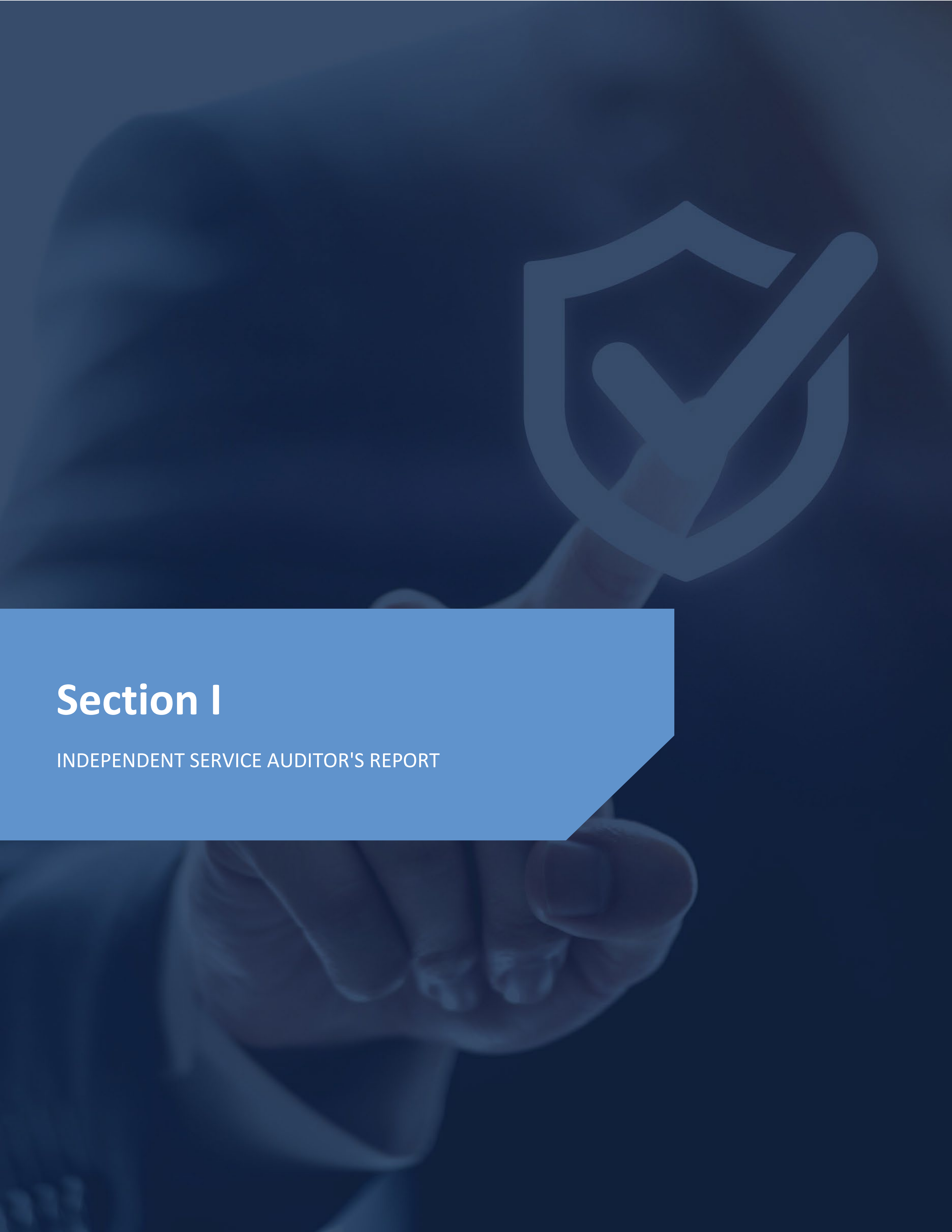
System and Organization Controls (SOC) 2 Type II Report on Management’s Description of its SiteCare

And the Suitability of the Design of Controls and Test of Operating Effectiveness of Controls Placed in Operation Relevant to Security Category

For the Period
December 10, 2024 to March 10, 2025

Together with Independent Service
Auditor’s Report

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

SiteCare, LLC

Scope

We have examined SiteCare, LLC's accompanying description of its SiteCare (system) titled "Description of SiteCare" throughout the period December 10, 2024 to March 10, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 10, 2024 to March 10, 2025, to provide reasonable assurance that SiteCare, LLC's service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

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

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

SiteCare, LLC 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 SiteCare, LLC's service commitments and system requirements were achieved. SiteCare, LLC has provided an assertion titled "Assertion of SiteCare, LLC's Management" (assertion) about the description and the suitability of the design and operating effectiveness of the controls stated therein. SiteCare, LLC is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description, based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in 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.

Description of Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents SiteCare, LLC's SiteCare (system) that was designed and implemented throughout the period December 10, 2024 to March 10, 2025 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period December 10, 2024 to March 10, 2025, to provide reasonable assurance that SiteCare, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of SiteCare, LLC's controls throughout the period.

c. The controls stated in the description operated effectively throughout the period December 10, 2024 to March 10, 2025, to provide reasonable assurance that SiteCare, LLC'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 SiteCare, LLC's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled “Description of Test of Controls and Results Thereof” is intended solely for the information and use of SiteCare, LLC; user entities of SiteCare, LLC’s SiteCare during some or all of the period December 10, 2024 to March 10, 2025, business partners of SiteCare, LLC subject to risks arising from interactions with the SiteCare, LLC’s processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

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

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

JohansonGroup LLP

Colorado Spring, Colorado
May 2, 2025

Section II

ASSERTION OF SITECARE, LLC MANAGEMENT

We have prepared the accompanying description of SiteCare, LLC's "Description of SiteCare" for the period December 10, 2024 to March 10, 2025, (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about SiteCare, LLC's SiteCare (system) that may be useful when assessing the risks arising from interactions with SiteCare, LLC's system, particularly information about system controls that SiteCare, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

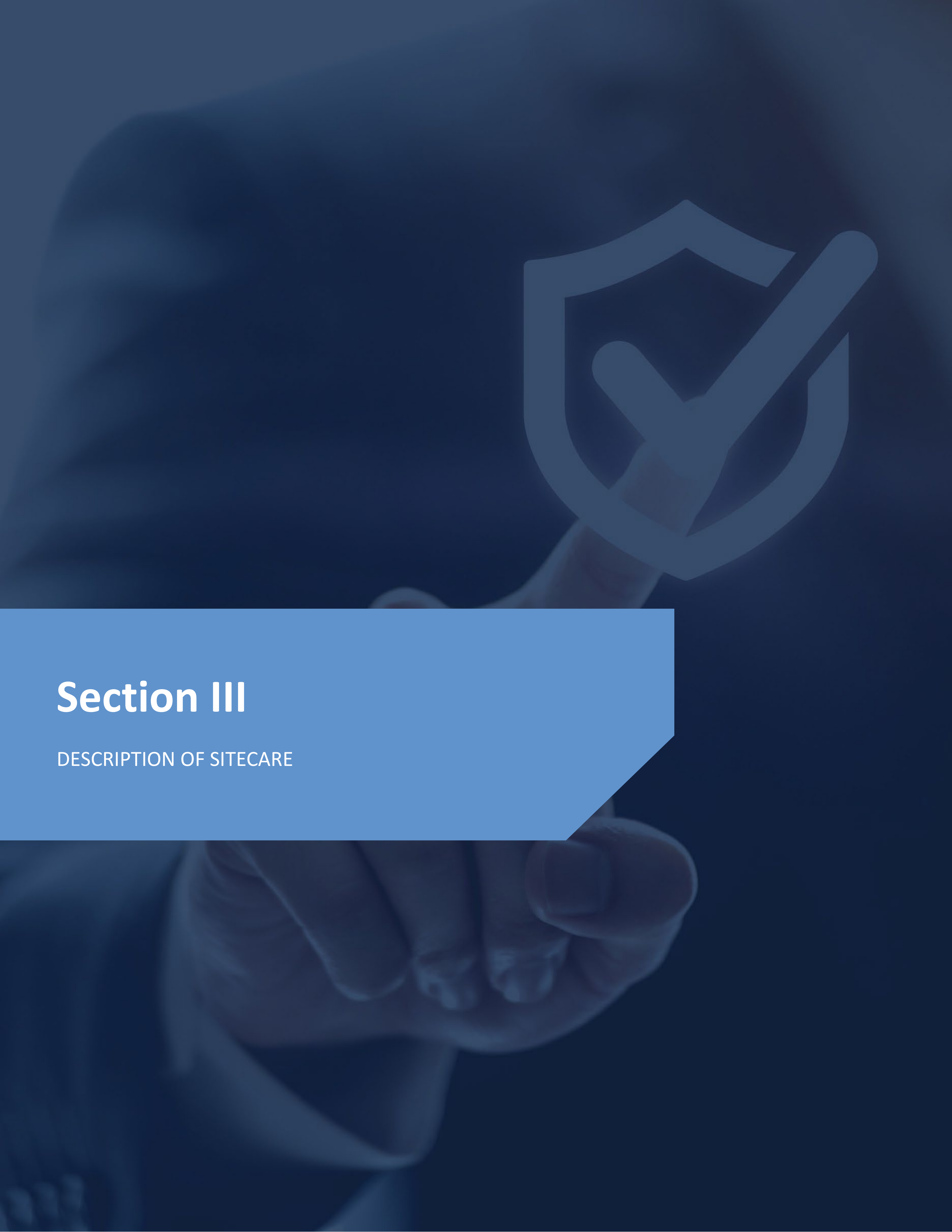
SiteCare, LLC uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SiteCare, LLC, to achieve SiteCare, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents SiteCare, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SiteCare, LLC's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. The description presents SiteCare, LLC's SiteCare (system) that was designed and implemented throughout the period December 10, 2024 to March 10, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 10, 2024 to March 10, 2025, to provide reasonable assurance that SiteCare, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of SiteCare, LLC's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period December 10, 2024 to March 10, 2025, to provide reasonable assurance that SiteCare, LLC'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 SiteCare, LLC's controls operated effectively throughout that period.

SiteCare, LLC Management
May 2, 2025



Section III

DESCRIPTION OF SITECARE

COMPANY BACKGROUND

Established in 2005, SiteCare's mission is to make business leaders proud and confident of their WordPress websites.

SiteCare serves industries including health care, publishing, technology, startups, manufacturing, and online retail.

DESCRIPTION OF SERVICES PROVIDED

SiteCare provides managed WordPress support, maintenance, security, and optimization services. SiteCare's scope of services includes:

- Proactive maintenance and updates
- Site health improvements and performance optimization
- Security monitoring and remediation
- Technical SEO improvements
- Rapid response support and communication
- System-generated monthly reports summarizing activities and site health

SiteCare works globally with clients in the United States, the United Kingdom, Canada, Australia, Sri Lanka, South Africa, and Germany. By relying on skilled WordPress professionals and established hosting partners, SiteCare ensures clients' WordPress websites are secure, performant, and optimized without unexpected disruptions. SiteCare's clients can focus on growing their businesses, entrusting the technical details to SiteCare and its vetted subservice organizations.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

SiteCare's processes, policies, and procedures are designed to deliver high-quality, reliable, and secure WordPress maintenance and support services. SiteCare's objectives are derived from its mission, user entity agreements, and applicable legal and regulatory requirements. Operational requirements are communicated internally and externally through policies, procedures, system design documentation, and customer agreements.

COMPONENTS OF THE SYSTEM

Infrastructure

SiteCare does not own or operate its own hosting platform or data center infrastructure. Instead, SiteCare's services are dependent on multiple third-party hosting and infrastructure providers. These subservice organizations deliver the networking, computing, and storage resources required for WordPress environments. SiteCare manages and supports client websites deployed on these external hosting platforms. While SiteCare's production infrastructure is hosted by subservice organizations such as DigitalOcean, SiteCare maintains responsibility for the configuration, security hardening, access control, and monitoring of client environments deployed within these platforms.

Subservice Organizations Providing Infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Backblaze	Backup Storage Provider	Store off-site backups securely with encryption and redundancy.
BlogVault	Backup & Recovery Tool	Provides daily remote backups and restoration capabilities for WordPress websites.
Cloudflare	CDN & Security Provider	Delivers content via CDN, mitigates DDoS attacks, and improves site speed and availability.

Digital Ocean	Infrastructure Provider	Cloud-based infrastructure for flexible and scalable server environments.
NordLayer	VPN Service Provider	Provides secure VPN access for remote employees to protect sensitive communications and transmissions.
Pagely	Infrastructure Provider	Provides managed WordPress hosting with dedicated VPS infrastructure, performance monitoring, and enterprise-grade support.
WP Engine	Infrastructure Provider	Delivers scalable managed WordPress hosting environments, including server resources, security hardening, and automated backups.

Note: All physical and virtual infrastructure components used to support SiteCare's services (e.g., servers, databases, and networks) are owned and managed by these subservice organizations. SiteCare relies on its SOC reports, contractual commitments, and industry certifications to ensure that its infrastructure meets the required standards for security, availability, and reliability.

Software

SiteCare uses various software tools and platforms—either provided by or running on the infrastructure of subservice organizations—to deliver and manage its services:

Primary Software		
Software	**Type**	**Purpose**
1Password	Credential Management	Manages, stores, and protects login credentials and secure notes.
Buddy	CI/CD Automation Tool	Handles pre-deployment and deployment tools, including CI/CD tooling for disruption-free delivery.
ClickUp	Workflow Management	Tracks tasks, change management workflows, and internal projects.
Drata	Compliance Automation	Monitors internal control effectiveness and assists with SOC 2 evidence and reporting.
Freshdesk	Helpdesk & Support Tool	Manages client communications, tickets, and support SLAs.
GitHub	Source Code Management	Stores version-controlled code, tracks changes, and supports CI/CD pipelines.
Google Workspace	SSO & Identity Tool	Provides SSO authentication, email, file storage, and employee identity management.
Kit	Email Marketing Platform	Sends and manages marketing emails and client communications.

Software Stack/System Components

Key Open-Source Software Stack: These components are installed and managed by SiteCare to deliver optimized WordPress experiences across client environments.

Primary Software		
Software	**Operating System**	**Purpose**
MySQL	Linux	Relational database management system used for storing and retrieving structured data for WordPress websites.
NGINX	Linux	High-performance web server and reverse proxy used for serving WordPress websites and optimizing traffic handling.
Redis	Linux	An in-memory data store is used to cache database queries and improve website performance.
Apache	Linux	Open-source web server used to deliver WordPress content to end users.
WordPress	Linux	A content management system (CMS) is used to build, manage, and optimize client websites.

People

SiteCare's team of 15 employees is organized into functional areas:

- Leadership (Governance and strategic oversight)
- Professional Services (Website maintenance, development, optimization)
- Account Management (Client experience, support, and liaison)
- Sales (Onboarding new clients and ensuring requirement alignment)
- Marketing (Branding, market positioning, and customer acquisition)

Data

SiteCare may handle:

- Basic personal details (name, email, contact details)
- Website access details (usernames, passwords, collaborator access)
- User activity within the software
- Other relevant data needed for ongoing website management and optimization

Basic Personal Details (name, email, contact details)

SiteCare handles basic personal details such as names, email addresses, and contact details to facilitate communication and provide managed services to clients. This data is processed through third-party subservice organizations that offer secure storage and processing capabilities. SiteCare ensures that personal details are encrypted in transit and at rest, leveraging the security features of these subservice organizations. Access to this data is limited to authorized personnel based on a role-based access model. SiteCare does not retain this information in its own infrastructure, and the storage and backup processes are managed by trusted subservice organizations to align with industry best practices.

Website Access Details (usernames, passwords, collaborator access)

Website access details are critical for SiteCare to perform maintenance, support, and optimization tasks for client websites. These credentials are securely managed through tools like 1Password, which is hosted on a third-party platform. SiteCare does not store or process these details directly but relies on the security mechanisms of subservice organizations to safeguard this information. Multi-factor authentication (MFA) is enforced where possible, and all access logs are periodically reviewed to ensure compliance with security protocols. This approach minimizes the risk of unauthorized access and ensures that sensitive access information remains protected.

User Activity Within Software

User activity data is collected to monitor system performance, troubleshoot issues, and optimize client websites. This data is stored and analyzed on third-party platforms such as ClickUp and Freshdesk, which provide detailed logs and reporting tools. SiteCare ensures that all activity data is transmitted securely and uses these insights strictly for improving service delivery. No user activity data is stored locally within SiteCare's infrastructure, and the subservice organizations hosting this data adhere to rigorous security and compliance standards.

Other Relevant Data Needed for Ongoing Website Management and Optimization

Additional data required for website management, such as performance metrics, SEO insights, and configuration settings, is processed using tools like Google Workspace and Cloudflare. This data is crucial for ensuring optimal website functionality and client satisfaction. SiteCare leverages the robust infrastructure of its subservice organizations to store and analyze this data securely. Encryption protocols, access controls, and periodic audits are implemented to maintain data integrity and confidentiality. SiteCare's reliance on subservice organizations ensures scalability and security, reducing potential vulnerabilities.

Each data type handled by SiteCare is managed with stringent controls and in partnership with industry-leading subservice organizations to ensure security, compliance, and efficiency.

PROCESSES, POLICIES, AND PROCEDURES

SiteCare's documented policies and procedures establish the requirements for managing its services. All staff must comply with these policies, which are readily available for reference. These policies detail responsibilities, security practices, operational guidelines, and compliance requirements.

Physical Security

All data managed by SiteCare is hosted by third-party subservice organizations. These subservice organizations operate secure data centers to which SiteCare employees do not have physical access. Currently, SiteCare does not maintain any physical office space, and all operations are conducted remotely by its distributed team. This approach further minimizes the risk of unauthorized physical access to data.

Logical Access

SiteCare employees are granted access to systems and infrastructure through a role-based access control system, ensuring least-privileged access for identified users. This approach simplifies provisioning and de-provisioning processes while maintaining consistent security standards across the organization.

SiteCare's operations rely entirely on cloud-based and SaaS platforms. Employee access is managed through accounts and permissions within these systems, with three levels of access defined:

- **Owner/Super Admin:** Has full control over the account, including billing, user management, and global settings.
- **Administrator:** Can manage users, roles, settings, and integrations within the platform.
- **Manager:** Can view and manage data or workflows for their assigned team or department.
- **Contributor:** Can create, edit, and collaborate on content or records they have access to.
- **Viewer:** Can view data and reports, but cannot make any changes.

Roles and permissions are reviewed annually by management to ensure adherence to least-privileged principles. Employees are primarily identified through their Google Workspace accounts, which function as SiteCare's corporate directory and Single Sign-On (SSO) provider. SiteCare's password policy requires employees and contractors to sign in to cloud tools using their Google Workspace accounts wherever supported. If Google Workspace sign-in is unavailable, employees must authenticate using a strong, unique password stored in an approved password manager.

SiteCare enforces multi-factor authentication (MFA) across its systems. All Google Workspace accounts require MFA, and other SaaS applications are configured to use MFA whenever possible. This ensures enhanced protection of sensitive resources.

The management team oversees employee onboarding, including provisioning Google Workspace and SaaS accounts based on role requirements. New hires must complete security training and enroll in MFA within 14 days of starting employment. Upon employee termination, management is responsible for deactivating all accounts within three days.

Employees may use company-provided computers or approved personal devices (Bring Your Own Device, BYOD) for their work. Employees are required to ensure that personal devices used for SiteCare work comply with SiteCare's security standards, including full-disk encryption, MDM software installation, up-to-date antivirus protection, regular software patching, and the use of secure network connections. All devices used for sensitive tasks must employ full-disk encryption and have endpoint monitoring tools installed. Company-owned devices are collected and de-provisioned or reassigned according to SiteCare's Asset Management policy. This process ensures secure handling of devices and accounts throughout their lifecycle.

Computer Operations – Backups

Customer data managed by SiteCare is backed up using tools provided by trusted subservice organizations, such as BlogVault and Backblaze. SiteCare leverages these platforms to ensure reliable backup processes. In the event of an exception or failure, SiteCare's team works with the subservice provider's systems to identify the root cause and re-run the backup job either immediately or as part of the next scheduled cycle.

Backup infrastructure is maintained entirely by subservice organizations, with SiteCare relying on their security measures to safeguard data. All backups are encrypted both in transit and at rest, utilizing the encryption technologies and key management systems of the respective subservice providers. Access to backups is restricted to authorized personnel through stringent access control mechanisms, ensuring that customer data remains secure and compliant with industry standards.

Computer Operations – Availability

SiteCare maintains an Incident Response Policy that empowers any employee to report potential security incidents promptly. Employees can initiate a response by notifying the internal operations team through multiple channels. The policy includes clear guidelines for classifying the severity of incidents to ensure appropriate prioritization and resolution.

External parties, such as clients and third-party security researchers, have access to secure communication channels for submitting encrypted incident reports and responsibly disclosing potential vulnerabilities to SiteCare's operations team.

Internally, SiteCare continuously monitors the health and performance of client websites and associated systems using tools like UptimeRobot, Cloudflare, and other monitoring platforms. This includes tracking uptime, site speed, and performance benchmarks, as well as identifying errors or anomalies. Critical incidents are escalated to an on-call operator who must acknowledge the issue within a defined timeframe. If no acknowledgment occurs, the incident is escalated to the broader operations team for immediate resolution. SiteCare does not control or guarantee the availability, uptime, or performance of third-party hosting platforms; clients are subject to the SLAs of the respective hosting provider.

SiteCare uses industry-standard vulnerability scanning tools to identify and address common security issues and vulnerabilities within the platforms it manages. An internal SLA is maintained to ensure timely remediation of identified issues, aligning with SiteCare's commitment to maintaining secure, available, and performant systems for its clients.

Compliance Management Platform

SiteCare uses Drata for compliance automation, monitoring, and documentation of internal controls. While Drata assists in providing continuous monitoring, SiteCare management remains ultimately responsible for the effective design, implementation, and operation of its internal controls. SiteCare regularly reviews Drata's SOC reports and performs risk assessments to ensure the accuracy and completeness of the information stored there.

System Operations

Because SiteCare leverages infrastructure from subservice organizations, these partners handle data center operations, redundancy, backups, and failover capabilities. SiteCare manages configuration settings, monitors site performance, and utilizes the backup and restoration services of the subservice organizations. System operations, including alert monitoring, incident management, and continuity planning, rely on both SiteCare's internal procedures and the capabilities of its subservice organizations.

Change Control

SiteCare adheres to documented Systems Development Life Cycle (SDLC) policies and procedures to guide the planning, documentation, and implementation of application and infrastructure changes. These policies outline comprehensive change control processes, including change requests, initiation procedures, documentation standards, development workflows, quality assurance testing, and necessary approvals.

SiteCare utilizes a ticketing system, such as ClickUp or Freshdesk, to document and manage change control procedures. Each change is tracked from initiation through implementation, with quality assurance (QA) and User Acceptance Testing (UAT) results attached to the associated change request. Development and testing activities are conducted in staging environments that are logically separated from production environments. Management reviews and approves changes prior to deployment, with all approvals recorded in the ticketing system to ensure accountability.

SiteCare employs version control software, such as GitHub, to maintain source code repositories. This software supports the full development lifecycle, including tracking changes made by developers, maintaining a history of code versions, and enabling rollback capabilities if needed. This structured approach ensures that all changes are thoroughly vetted and documented, minimizing risks and supporting reliable service delivery for SiteCare's clients.

Data Communications

SiteCare relies on subservice organizations such as Digital Ocean, Pagely, and WP Engine to manage its production infrastructure. These providers simplify network configuration and operations by offering secure, scalable solutions with built-in protections. Logical network configurations are secured using advanced firewalls, with ingress to SiteCare-managed environments limited to HTTPS connections through designated endpoints.

Subservice organizations automate the provisioning and de-provisioning of infrastructure resources to ensure high availability. For example, if a server or container experiences a failure, it is automatically replaced, maintaining seamless operations without requiring manual intervention.

To ensure robust security, SiteCare engages external security services for regular vulnerability scanning and periodic penetration testing. Any vulnerabilities identified are addressed promptly through SiteCare's established incident response and change management processes.

SiteCare does not maintain a corporate network or intranet. However, it does require VPN usage to access critical systems. It also utilizes cloud-based SaaS tools accessible via the public internet and secured through encrypted TLS connections. This approach ensures flexibility and security while reducing the complexity of traditional network management.

Data Governance

Data governance processes focus on how data is classified, handled, and protected. While SiteCare manages and accesses client data, the physical storage, security, and backups are performed by subservice organizations. SiteCare's policies ensure the appropriate use, handling, and protection of this data while relying on third-party hosting platforms for underlying data security controls.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the managed WordPress support, maintenance, and optimization services performed by SiteCare. This report does not include the hosting and infrastructure services provided by subservice organizations, including Digital Ocean.

APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage, and ii. systems that use electronic information to process, transmit, transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

SiteCare's commitment to ethical standards underpins its control environment.

- Policies and codes of conduct outline ethical expectations for employees.
- Employees acknowledge their understanding of these policies during onboarding.
- Background checks are performed as part of the hiring process.
- Confidentiality agreements safeguard client data.

Commitment to Competence

SiteCare defines and supports competence through:

- Clear role descriptions and requisite skill requirements.
- Ongoing training to maintain proficiency.

Management's Philosophy and Operating Style

SiteCare's management focuses on balancing operational growth with robust data protection practices. Regular management reviews ensure compliance with industry standards and alignment with service objectives.

Organizational Structure and Assignment of Responsibility

SiteCare maintains a structured organization where roles and responsibilities are well-defined. Organizational charts are updated and communicated to employees to ensure clarity in reporting and authority.

Human Resource Policies and Practices

SiteCare ensures operational efficiency through sound HR practices, including:

- Confidentiality agreements and employee handbooks are signed during onboarding.
- Regular performance evaluations.
- Documented termination procedures to secure access controls.

RISK ASSESSMENT PROCESS

SiteCare's risk assessment process identifies and mitigates risks affecting service delivery. A risk register tracks identified risks, evaluates their impact, and guides corrective actions. This process is reviewed annually.

SiteCare uses Drata for risk assessment, monitoring, and documentation of internal controls. While Drata assists in providing continuous monitoring, SiteCare management remains ultimately responsible for the effective design, implementation, and operation of its internal controls. SiteCare regularly reviews Drata's SOC reports and performs risk assessments to ensure the accuracy and completeness of the information stored there.

INFORMATION AND COMMUNICATION SYSTEMS

SiteCare uses tools such as Slack, Google Workspace, and Freshdesk to facilitate internal and external communication. These systems support secure data exchange and operational transparency.

MONITORING CONTROLS

SiteCare continuously monitors control effectiveness using Drata and adapts it to changing conditions. Quality assurance processes and internal reviews ensure compliance and identify areas for improvement.

On-Going Monitoring

Management conducts regular monitoring and corrective actions based on quality assurance results. Issues are escalated as needed to address deviations from expected standards.

Reporting Deficiencies

SiteCare documents monitoring outcomes in Drata and escalate critical issues promptly. Corrective actions are tracked and reviewed in annual risk meetings.

CHANGES TO THE SYSTEM IN THE LAST 12 MONTHS

No significant changes have occurred to SiteCare's service delivery systems in the past year.

INCIDENTS IN THE LAST 12 MONTHS

No significant incidents affecting service delivery were reported during the review period.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria/Security were applicable to SiteCare's services.

SUBSERVICE ORGANIZATIONS

SiteCare relies on several trusted subservice organizations to deliver high-quality managed WordPress support, maintenance, and optimization services. These organizations provide the infrastructure and tools that underpin SiteCare's operations, including hosting, security, backup, and monitoring services. The effective functioning of SiteCare's systems is contingent on the controls implemented by these subservice organizations.

Roles and Responsibilities of Subservice Organizations

The following subservice organizations provide critical services to SiteCare:

- **1Password:** Manages and secures team credentials, passwords, and sensitive client access information.
- **Backblaze:** Supplies secure cloud storage for off-site backup retention with encryption and redundancy.
- **BlogVault:** Offers automated WordPress backup and restore services to protect client site data.

- **Buddy:** Provides continuous integration and deployment (CI/CD) automation for WordPress websites, enabling efficient and reliable code testing, builds, and deployments across staging and production environments.
- **ClickUp:** Enables project and task management, including documentation of change requests and internal workflows.
- **Cloudflare:** Provides content delivery, DDoS mitigation, DNS management, and performance optimization for WordPress websites.
- **Digital Ocean:** Deliver managed WordPress hosting platforms, including server management, storage, and scalable infrastructure to support client websites.
- **Drata:** Automates monitoring of internal controls, manages audit evidence, and supports SOC 2 compliance efforts.
- **Freshdesk:** Handles customer support requests, tracks response times, and maintains client communication logs.
- **GitHub:** Hosts source code repositories and version control for managing website development and deployments.
- **Google Workspace:** Provides email, document collaboration, and Single Sign-On (SSO) for identity and access management.
- **Kit:** Manages email marketing and newsletter distribution to SiteCare clients and subscribers.
- **NordLayer:** Delivers secure remote VPN access for staff working with sensitive systems and client environments.
- **Pagely:** Provides managed WordPress hosting with scalable VPS infrastructure, uptime monitoring, advanced caching, and enterprise-grade technical support for performance-focused environments.
- **WP Engine:** Offers secure, high-performance managed WordPress hosting environments with built-in caching, daily backups, and automated WordPress core updates.

Each subservice organization implements its own internal controls, which are integral to meeting the trust services criteria outlined in this report. SiteCare assumes that these organizations follow industry best practices for security, availability, and confidentiality as evidenced by their SOC 2 reports, certifications, or other attestations.

Monitoring Subservice Organizations

SiteCare takes a proactive approach to ensure that subservice organizations meet the required standards:

1. **Regular Reviews:** SiteCare periodically reviews SOC 2 reports, certifications, and audit findings from subservice organizations to verify that their controls align with trust service criteria.
2. **Vendor Communication:** SiteCare holds regular discussions with vendors to address operational updates, security enhancements, and any incidents that may impact services.
3. **Contractual Agreements:** SiteCare maintains service-level agreements (SLAs) with subservice organizations to outline mutual responsibilities and expectations.
4. **Issue Escalation:** If an issue arises that impacts service delivery, SiteCare works closely with the subservice organization to ensure timely resolution.

Examples of Complementary Subservice Organization Controls

Certain controls are implemented by subservice organizations to support SiteCare’s service delivery objectives, including:

- **Physical Security:** Data centers operated by subservice organizations are equipped with access controls, surveillance systems, and environmental protections to prevent unauthorized access and ensure operational reliability.
- **Redundancy and Availability:** Infrastructure provided by subservice organizations includes failover mechanisms, uninterruptible power supplies (UPS), and geographical redundancy to minimize service disruptions.
- **Data Protection:** Subservice organizations implement encryption for data in transit and at rest, as well as robust backup and recovery processes to ensure data integrity and confidentiality.

The following subservice organization controls should be implemented by Digital Ocean, Pagely, and WP Engine to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization	Category	Criteria	Control
DigitalOcean	Security	CC6.4	• The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. • Requests for new and modified workforce member physical access to the DigitalOcean collocated data centers are documented in a ticketing system by a member of the data center operations team. • Data center operations workforce personnel document workforce member physical access revocation to the DigitalOcean data centers in a ticketing system as a component of the termination process. • The data center operations team reviews the collocated data center access listings at least annually.
Pagely	Security	CC6.4	• AWS is responsible for restricting physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers where the entity's system resides.
WP Engine	Security	CC6.4	• Physical access to data centers is approved by an authorized individual. • Physical access is revoked within 24 hours of the employee or vendor record being deactivated. • Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. • Physical access points to server locations are recorded by closed-circuit television cameras (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations. • Physical access points to server locations are managed by electronic access control devices. • Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Shared Responsibility Model

While subservice organizations provide the underlying infrastructure, SiteCare ensures proper configuration, management, and monitoring of the services it delivers to clients. This shared responsibility model ensures:

- **SiteCare's Role:** Configuring and managing client environments, monitoring performance, and addressing incidents promptly.
- **Subservice Organizations' Role:** Maintaining the physical and virtual infrastructure that supports SiteCare's operations.

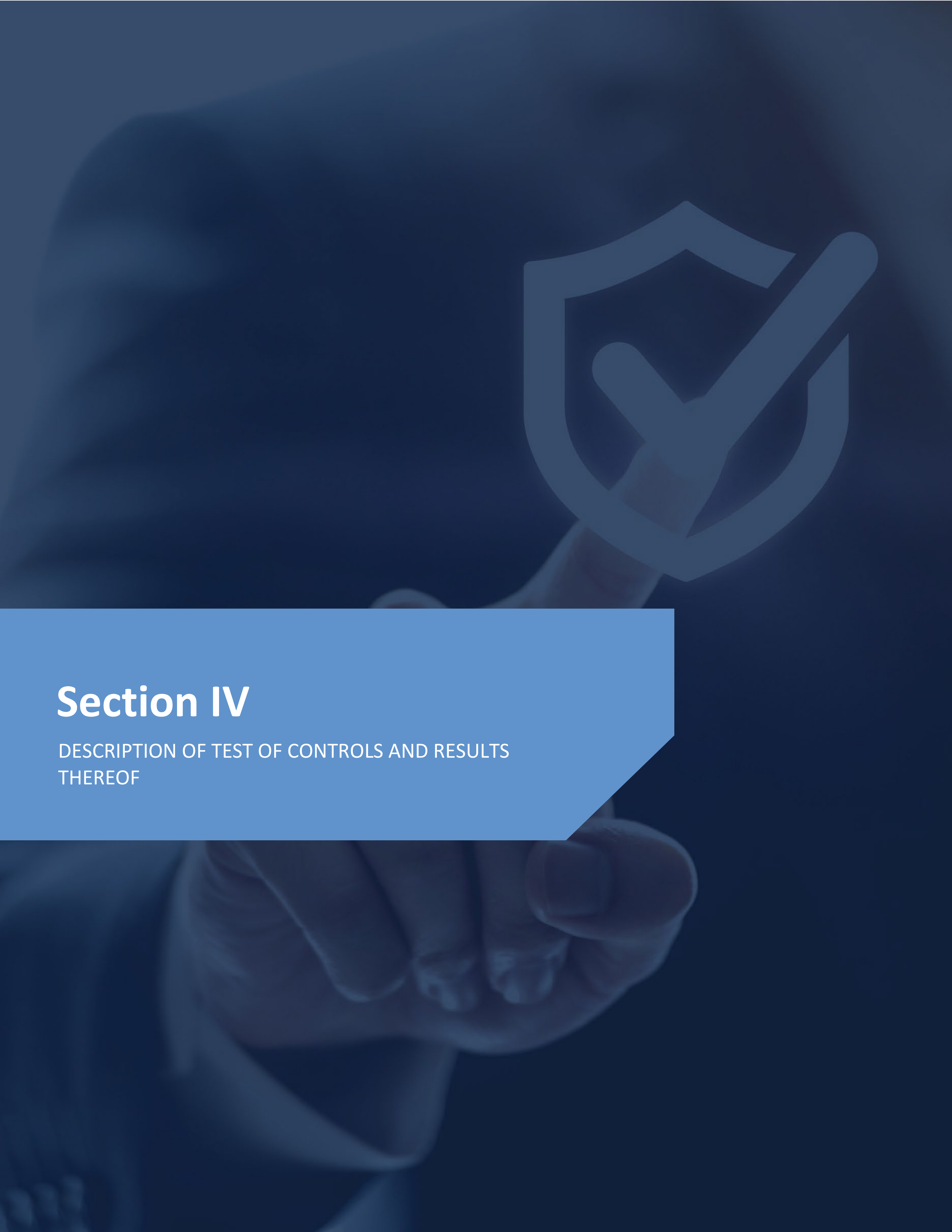
This collaborative approach enables SiteCare to deliver secure, reliable, and high-performing services to its clients while leveraging the strengths of its subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

SiteCare's clients are expected to implement controls that complement SiteCare's operations, including:

1. User entities are responsible for understanding and complying with their contractual obligations to SiteCare.
2. Ensuring proper use of SiteCare services by their personnel.
3. Maintaining disaster recovery plans for hosted environments.
2. Promptly notify SiteCare of any security incidents.

All client expectations are outlined in the SiteCare Terms of Service: https://sitecare.com/legal-070125/



Section IV

DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and SiteCare, LLC-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if SiteCare, LLC’s controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, throughout the period December 10, 2024 to March 10, 2025.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of SiteCare, LLC activities and operations, and inspection of SiteCare, LLC documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all SiteCare, LLC controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 1.0 - Control Environment			
CC 1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	SiteCare maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Code of Conduct to determine that SiteCare, LLC maintains a documented policy. Eligible personnel are required to acknowledge SiteCare's policy during onboarding and annually thereafter.	No exceptions noted.
	Company policies are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's security policies to determine that they are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
	Background checks are conducted on eligible personnel (employees and third parties as deemed necessary by the organization) prior to hire as permitted by local laws.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed background checks to determine that they are conducted on eligible personnel (employees and third parties as deemed necessary by the organization) prior to hire as permitted by local laws.	No exceptions noted.
	Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	Inspected SiteCare, LLC's internal communication channels to determine that these are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Management conducts performance evaluations for eligible personnel at least annually.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed performance evaluation to determine that management conducts evaluations for eligible personnel at least annually.	No exceptions noted.
	Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.	Inspected SiteCare, LLC's Mutual Non-Disclosure Agreement to determine that personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.	No exceptions noted.
	Personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	Inspected SiteCare, LLC's Confidentiality & Proprietary Rights Agreement to determine that personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	No exceptions noted.
	SiteCare has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inspected SiteCare, LLC's Disciplinary Process to determine it has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	No exceptions noted.
CC 1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected SiteCare, LLC's Board of Directors CVs to determine that the company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed.	No exceptions noted.
CC 1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected SiteCare, LLC's board charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No exceptions noted.
	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	Inspected SiteCare, LLC's organizational chart to determine that it is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Management has established and documented roles and responsibilities for personnel, including responsibilities for the implementation of the risk management and compliance program (e.g., security, privacy, AI, etc.) and oversight activities.	Inspected SiteCare, LLC's Information Security Policy to determine the roles and responsibilities of personnel, including responsibilities for implementation of the risk management and compliance program (e.g., security, privacy, AI, etc.), and oversight activities.	No exceptions noted.
	Personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	Inspected SiteCare, LLC's Confidentiality & Proprietary Rights Agreement to determine that personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	No exceptions noted.
	SiteCare has appointed and documented the responsibilities of an individual (e.g., data protection officer) responsible for developing, implementing, maintaining, and monitoring an organization-wide governance and privacy program and acting as a point of contact to authorities and data subjects to ensure compliance with all applicable laws and regulations regarding the processing of PII.	Inspected SiteCare, LLC's Chief of Staff as Designated Data Protection Officer to determine that it has appointed and documented responsibilities of an individual (e.g., data protection officer) responsible for developing, implementing, maintaining, and monitoring an organization-wide governance and privacy program and acting as a point of contact to authorities and data subjects to ensure compliance with all applicable laws and regulations regarding the processing of PII.	No exceptions noted.
CC 1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Management conducts performance evaluations for eligible personnel at least annually.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed performance evaluation to determine that management conducts evaluations for eligible personnel at least annually.	No exceptions noted.
	SiteCare maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Code of Conduct to determine that SiteCare maintains a documented policy. Eligible personnel are required to acknowledge SiteCare's policy during onboarding and annually thereafter.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed security training to determine that the company has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	No exceptions noted.
	Management evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Confidentiality & Proprietary Rights Agreement to determine that SiteCare evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	No exceptions noted.
	SiteCare has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected SiteCare, LLC's sample job description to determine that the company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
	Developers are required to complete secure code development training at least once every 12 months, including training on software security relevant to their job function and development languages, secure software design and secure coding techniques, and how to use tools for detecting vulnerabilities in software if these are used in the organization.	Inspected SiteCare, LLC's training completion certificate to determine that developers are required to complete secure code development training at least once every 12 months, including training on software security relevant to their job function and development languages, secure software design, and secure coding techniques, and how to use tools for detecting vulnerabilities in software if these are used in the organization.	No exceptions noted.
	SiteCare conducts periodic phishing simulations as part of the company's security awareness initiatives.	Inspected SiteCare, LLC's phishing test report to determine that it conducts periodic phishing simulations as part of the company's security awareness initiatives.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	Inspected SiteCare, LLC's Privacy Training and Security Training to determine that it has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	No exceptions noted.
CC 1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Management conducts performance evaluations for eligible personnel at least annually.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed performance evaluation to determine that management conducts evaluations for eligible personnel at least annually.	No exceptions noted.
	SiteCare maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Code of Conduct to determine that SiteCare, LLC maintains a documented policy. Eligible personnel are required to acknowledge SiteCare's policy during onboarding and annually thereafter.	No exceptions noted.
	Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	Inspected SiteCare, LLC's internal communication channels to determine that these are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	No exceptions noted.
	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	Inspected SiteCare, LLC's organizational chart to determine that it is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	No exceptions noted.
	SiteCare has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inspected SiteCare, LLC's Disciplinary Process to determine it has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 2.0 - Communication and Information			
CC 2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	SiteCare has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control.	Inspected SiteCare, LLC's Information Security Policy that SiteCare has defined and documented policy and other topic-specific policies as needed to support the functioning of internal control.	No exceptions noted.
	A centralized asset register is maintained for physical, cloud, and other assets that include descriptive attributes for asset accountability such as owner, description, location, and other attributes based on the type of asset. The asset inventory is reviewed and updated at periodic intervals and/or updated as needed (e.g., as a result of new purchases, installations, removals, system changes, etc.).	Inspected SiteCare, LLC's Asset Inventory to determine that the company's centralized asset register is maintained for physical, cloud, and other assets that include descriptive attributes for asset accountability such as owner, description, location, and other attributes based on the type of asset. The asset inventory is reviewed and updated at periodic intervals and/or updated as needed (e.g., as a result of new purchases, installations, removals, system changes, etc.).	No exceptions noted.
	Company policies are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's security policies to determine that they are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
	Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	Inspected SiteCare, LLC's Policy packet to determine that company management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the security policy review was conducted outside of the review period.
	SiteCare has established a data classification policy in order to identify the types of information stored or processed by the entity and the protection measures that are required for each.	Inspected SiteCare, LLC's Data Classification Policy to determine that SiteCare has established a data classification policy in order to identify the types of information stored or processed by the entity and the protection measures that are required for each.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
CC 2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	Inspected SiteCare, LLC's meeting minutes to determine that the company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the meetings were conducted outside of the review period.
	Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	Inspected SiteCare, LLC's Policy packet to determine that the company's management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the security policy review was conducted outside of the review period.
	SiteCare maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Code of Conduct to determine that SiteCare, LLC maintains a documented policy. Eligible personnel are required to acknowledge SiteCare's policy during onboarding and annually thereafter.	No exceptions noted.
	SiteCare has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed security training to determine that the company has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Company policies are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's security policies to determine that they are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
	Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	Inspected SiteCare, LLC's internal communication channels to determine that these are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable.	No exceptions noted.
	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	Inspected SiteCare, LLC's organizational chart to determine that it is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.	No exceptions noted.
	SiteCare has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected SiteCare, LLC's sample job description to determine that the company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
	Personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	Inspected SiteCare, LLC's Confidentiality & Proprietary Rights Agreement to determine that personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.).	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Developers are required to complete secure code development training at least once every 12 months, including training on software security relevant to their job function and development languages, secure software design and secure coding techniques, and how to use tools for detecting vulnerabilities in software if these are used in the organization.	Inspected SiteCare, LLC's training completion certificate to determine that developers are required to complete secure code development training at least once every 12 months, including training on software security relevant to their job function and development languages, secure software design, and secure coding techniques, and how to use tools for detecting vulnerabilities in software if these are used in the organization.	No exceptions noted.
	SiteCare's security awareness program includes multiple methods of communicating awareness and educating personnel, such as newsletters, web-based training, in-person training, team meetings, phishing simulations, etc. Periodic security updates are provided to personnel through these multiple methods of communication.	Inspected SiteCare, LLC's Periodic Security Updates to determine that the security awareness program includes multiple methods of communicating awareness and educating personnel, such as newsletters, web-based training, in-person training, team meetings, phishing simulations, etc. Periodic security updates are provided to personnel through these multiple methods of communication.	No exceptions noted.
	SiteCare has established and documented records of processing activity (ROPA), which includes descriptions of the lawful collection and use of PII as well as the specific purposes for which PII is processed.	Inspected SiteCare, LLC's processing activity to determine that it has established and documented records of activity, which include descriptions of the lawful collection and use of PII as well as the specific purposes for which PII is processed.	No exceptions noted.
	SiteCare conducts periodic phishing simulations as part of the company's security awareness initiatives.	Inspected SiteCare, LLC's phishing test report to determine that it conducts periodic phishing simulations as part of the company's security awareness initiatives.	No exceptions noted.
	SiteCare has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	Inspected Privacy Training's privacy and security training to determine that it has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare provides user guides, help articles, system documentation, and other mechanisms for users to share information about the design and operation of the system and its boundaries. The information provided includes functional and non-functional requirements related to system processing and information specifications required to support the use of the system.	Inspected SiteCare, LLC's Help Center Page to determine that it provides user guides, help articles, system documentation, or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and non-functional requirements related to system processing and information specifications required to support the use of the system.	No exceptions noted.
	Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	Inspected SiteCare, LLC's defined company objectives to determine that management has objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	No exceptions noted.
CC 2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	SiteCare maintains a publicly available privacy policy/notice.	Inspected SiteCare, LLC's privacy policy to determine that SiteCare, LLC maintains a publicly available privacy policy/notice.	No exceptions noted.
	Master service agreements outlining specific requirements are executed with enterprise customers or when the standard terms of service may not apply.	Inspected SiteCare, LLC's Terms of Service or MAS to determine that SiteCare, LLC's master service agreements outlining specific requirements are executed with enterprise customers or when the standard terms of service may not apply.	No exceptions noted.
	SiteCare provides external communication mechanisms to customers (e.g., communication features, support portal, external ticketing system, etc.) to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer support tickets are responded to by the support team within defined SLAs.	Inspected SiteCare, LLC's website security page to determine that the company provides external communication mechanisms to customers (e.g., communication features, support portal, external ticketing system, etc.) to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer support tickets are responded to by the support team within defined SLAs.	No exceptions noted.
	SiteCare communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company websites, etc. SiteCare provides notification to relevant parties of any changes to service commitments and system requirements.	Inspected SiteCare, LLC's Terms of Service to determine the company's service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. SiteCare provides notification to relevant parties of any changes to service commitments and system requirements.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare maintains publicly available terms of service for the use of the system. All users must agree to the terms of service prior to using the system.	Inspected SiteCare, LLC's terms of service to determine that it maintains publicly available terms of service for the use of the system. All users must agree to the terms of service prior to using the system.	No exceptions noted.
	Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.	Inspected SiteCare, LLC's Mutual Non-Disclosure Agreement to determine that personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.	No exceptions noted.
	SiteCare shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information.	Inspected SiteCare, LLC's vendor and data processing agreement to determine that it shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information.	No exceptions noted.
	SiteCare provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.).	Inspected SiteCare, LLC's support email to determine that it provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.).	No exceptions noted.
	The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	Inspected SiteCare, LLC's meeting minutes to determine that the company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the meetings were conducted outside of the review period.
	SiteCare notifies customers of any intended changes (including additions and replacements) in subprocessors that process PII so that customers have an opportunity to object to such changes.	Inspected SiteCare, LLC's customer communication of subprocessor changes to determine that the company notifies customers of any intended changes (including additions and replacements) in subprocessors that process PII so that customers have an opportunity to object to such changes.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare provides user guides, help articles, system documentation, and other mechanisms for users to share information about the design and operation of the system and its boundaries. The information provided includes functional and non-functional requirements related to system processing and information specifications required to support the use of the system.	Inspected SiteCare, LLC's Help Center Page to determine that it provides user guides, help articles, system documentation, or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and non-functional requirements related to system processing and information specifications required to support the use of the system.	No exceptions noted.
	SiteCare communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors on the company website or data processing agreement, etc.). SiteCare obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).	Inspected SiteCare, LLC's Kit Data Processing Agreement to determine that it communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). SiteCare obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).	No exceptions noted.
CC 3.0 - Risk Assessment			
CC 3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company websites, etc. SiteCare provides notification to relevant parties of any changes to service commitments and system requirements.	Inspected SiteCare, LLC's agreeing to terms of service to determine the company's service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. SiteCare provides notification to relevant parties of any changes to service commitments and system requirements.	No exceptions noted.
	Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	Inspected SiteCare, LLC's defined company objectives to determine that management has objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	No exceptions noted.
CC 3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected SiteCare, LLC's vulnerability scan to determine that SiteCare, LLC conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel, and vulnerabilities are tracked to resolution in accordance with company policies.	No exceptions noted.
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare maintains a vendor/third-party register that includes a description of each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing, or managing information assets are reviewed to validate they address all relevant requirements prior to execution.	Inspected SiteCare, LLC's vendor agreement to determine that SiteCare, LLC maintains a vendor/third party register that includes a description for each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing, or managing information assets are reviewed to validate that they address all relevant requirements prior to execution.	No exceptions noted.
	SiteCare obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.), and SiteCare's requirements. Results of the review and action items, if any, are documented.	Inspected SiteCare, LLC's Directory of key vendors and verified the use of automated continuous control monitoring to determine that SiteCare obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.), and SiteCare's requirements. Results of the review and action items, if any, are documented.	No exceptions noted.
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
	SiteCare performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures, or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities including action items are documented.	Inspected SiteCare, LLC's vendor due diligence discovery to determine that SiteCare, LLC performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures, or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities, including action items, are documented.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	Inspected SiteCare, LLC's defined company objectives to determine that management has objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.	No exceptions noted.
CC 3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
	SiteCare performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology.	Inspected SiteCare, LLC's fraud risk assessment to determine that the company performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
CC 4.0 - Monitoring Activities			
CC 4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	SiteCare conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected SiteCare, LLC's vulnerability scan to determine that SiteCare, LLC conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel, and vulnerabilities are tracked to resolution in accordance with company policies.	No exceptions noted.
	Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected SiteCare, LLC's system access review to determine that SiteCare, LLC management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Production systems and resources are monitored, and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	Inspected SiteCare, LLC's system access monitoring to determine that production systems and resources are monitored, and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
CC 4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.
	The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	Inspected SiteCare, LLC's meeting minutes to determine that the company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the meetings were conducted outside of the review period.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 5.0 - Control Activities			
CC 5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	Access to make changes in production environments is restricted to authorized personnel in accordance with the segregation of duties principles and the company's documented policies and procedures.	Inspected SiteCare, LLC's change deployers and verified the use of automated continuous control monitoring to determine that Access to make changes in production environments is restricted to authorized personnel in accordance with the segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's data access to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	Inspected SiteCare, LLC's risk assessment to determine that SiteCare conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact of each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. The results of the risk assessment are documented.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the risk assessment was conducted outside of the review period
	SiteCare conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected SiteCare, LLC's vulnerability scan to determine that SiteCare, LLC conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel, and vulnerabilities are tracked to resolution in accordance with company policies.	No exceptions noted.
	SiteCare has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's completed security training to determine that the company has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.	No exceptions noted.
	Company policies are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's security policies to determine that they are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
	SiteCare's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected SiteCare, LLC's risk treatment plan to determine that the company's management has a documented plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
	Administrative or privileged access to systems and resources is restricted to authorized personnel.	Inspected SiteCare, LLC's administrative users to determine that privileged access to systems and resources is restricted to authorized personnel.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's data access to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
	SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected SiteCare, LLC's Information Security Policy to determine that SiteCare uses compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
	Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	Inspected SiteCare, LLC's Change Management Policy to determine that changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	No exceptions noted.
CC 5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	SiteCare has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control.	Inspected SiteCare, LLC's Information Security Policy that SiteCare has defined and documented policy and other topic-specific policies as needed to support the functioning of internal control.	No exceptions noted.
	SiteCare maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Obtained a sample of current employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Code of Conduct to determine that SiteCare, LLC maintains a documented policy. Eligible personnel are required to acknowledge SiteCare's policy during onboarding and annually thereafter.	No exceptions noted.
	SiteCare has a documented disaster recovery plan that outlines roles, responsibilities, and detailed procedures for the recovery of systems in the event of a disaster scenario.	Inspected SiteCare, LLC's Disaster Recovery Plan to determine that it has a documented disaster recovery plan that outlines roles, responsibilities, and detailed procedures for the recovery of systems in the event of a disaster scenario.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Company policies are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's security policies to determine that they are accessible to all employees and, as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
	Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	Inspected SiteCare, LLC's Policy packet to determine that the company’s management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the security policy review was conducted outside of the review period.
	SiteCare has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's Employees' Acceptance of the Policy to determine that it has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.	No exceptions noted.
	SiteCare has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected SiteCare, LLC's Business Continuity Plan to determine that SiteCare has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	No exceptions noted.
	SiteCare has a documented policy that establishes requirements for the use of cryptographic controls.	Inspected SiteCare, LLC's Encryption Policy to determine that SiteCare has a documented policy that establishes requirements for the use of cryptographic controls.	No exceptions noted.
	SiteCare has established and documented a policy that outlines requirements for the management and tracking of company assets.	Inspected SiteCare, LLC's Asset Management Policy to determine that SiteCare has established and documented a policy that outlines requirements for the management and tracking of company assets.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected SiteCare, LLC's Vulnerability Management Policy to determine that SiteCare has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
	SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	Inspected SiteCare, LLC's Risk Assessment Policy to determine that SiteCare has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance.	No exceptions noted.
CC 6.0 - Logical and Physical Access			
CC 6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A password manager is installed on all company-managed devices.	Inspected SiteCare, LLC's password manager to determine that it is installed on all company-managed devices.	No exceptions noted.
	Hard-disk encryption is enabled on all company-managed devices.	Inspected SiteCare, LLC's hard disk encryption to determine that it is enabled on all company-managed devices.	No exceptions noted.
	SiteCare has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected SiteCare, LLC's Password Configurations to determine that SiteCare, LLC has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	No exceptions noted.
	A centralized asset register is maintained for physical, cloud, and other assets that include descriptive attributes for asset accountability such as owner, description, location, and other attributes based on the type of asset. The asset inventory is reviewed and updated at periodic intervals and/or updated as needed (e.g., as a result of new purchases, installations, removals, system changes, etc.).	Inspected SiteCare, LLC's Asset Inventory to determine that the company's centralized asset register is maintained for physical, cloud, and other assets that include descriptive attributes for asset accountability, such as owner, description, location, and other attributes based on the type of asset. The asset inventory is reviewed and updated at periodic intervals and/or updated as needed (e.g., as a result of new purchases, installations, removals, system changes, etc.).	No exceptions noted.
	Authentication to systems requires the use of multi-factor authentication.	Inspected SiteCare, LLC's Multi-Factor Authentication and verified the use of automated continuous control monitoring to determine that authentication to systems requires the use of multi-factor authentication.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Data at rest is encrypted using strong cryptographic algorithms.	Inspected SiteCare, LLC's infrastructure data encryption to determine that data at rest is encrypted using strong cryptographic algorithms.	No exceptions noted.
	SiteCare has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.).	Inspected SiteCare, LLC's Password Configuration to determine that the company has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.).	No exceptions noted.
	Unique user IDs are used for authentication to systems.	Inspected SiteCare, LLC's infrastructure and version control accounts, and verified the use of automated continuous control monitoring to determine that unique user IDs are used for authentication to systems.	No exceptions noted.
	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's data access to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
	SiteCare has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.).	Inspected SiteCare, LLC's hardening standards that are in place to determine that SiteCare has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.).	No exceptions noted.
	Administrative or privileged access to systems and resources is restricted to authorized personnel.	Inspected SiteCare, LLC's administrative users to determine that privileged access to systems and resources is restricted to authorized personnel.	No exceptions noted.
	Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.).	Inspected SiteCare, LLC's remote access to production systems to determine that it is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.).	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has implemented segregation mechanisms so that customers cannot impact or access the data or resources of other customers.	Inspected SiteCare, LLC's Data Storage and Data Security in Freshdesk to determine that they have implemented segregation mechanisms so that customers cannot impact or access the data or resources of other customers.	No exceptions noted.
	System and physical access are revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	Obtained a sample of the list of terminated employees by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's access is revoked to determine that system and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	No exceptions noted.
	Root password authentication to production resources (e.g., virtual machines, containers, etc.) is disabled and only allowed under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	Inspected SiteCare, LLC's root password login disabled to determine that root password authentication to production resources (e.g., virtual machines, containers, etc.) is disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	No exceptions noted.
	Key-management policies and procedures are documented and implemented including the generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	Inspected SiteCare, LLC's Encryption Policy to determine that key-management policies and procedures are documented and implemented, including the generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	No exceptions noted.
	SiteCare retires, replaces, or destructs cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations.	Inspected SiteCare, LLC's Encryption Policy to determine that SiteCare, LLC retires, replaces, or destructs cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations.	No exceptions noted.
	SiteCare restricts access to system components and data to only those individuals whose job requires such access.	Inspected SiteCare, LLC's Administrative Users to determine that SiteCare, LLC restricts access to system components and data to only those individuals whose job requires such access.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 30 minutes or until the identity of the user is confirmed (for example, by a system administrator).	Inspected SiteCare, LLC's Account Lockout to determine that SiteCare, LLC has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 30 minutes or until the identity of the user is confirmed (for example, by a system administrator).	No exceptions noted.
	System configuration settings are in place to prevent password reuse. Individuals are not allowed to submit a new password that is the same as any of the last four passwords used, at a minimum.	Inspected SiteCare, LLC's Password History Enforcement to determine that SiteCare, LLC system configuration settings are in place to prevent password reuse. Individuals are not allowed to submit a new password that is the same as any of the last four passwords used, at a minimum.	No exceptions noted.
	SiteCare has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected SiteCare, LLC's password policy to determine that SiteCare has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise, along guidance on how to report the incident, etc.	No exceptions noted.
	Group-shared or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user.	Inspected SiteCare, LLC's shared account management to determine that group-shared or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user.	No exceptions noted.
	SiteCare uses tags to assign metadata to cloud resources to facilitate the identification, inventory, and classification of virtual assets.	Inspected SiteCare, LLC's cloud asset tagging system to determine that it uses tags to assign metadata to cloud resources to facilitate identification, inventory, and classification of virtual assets.	No exceptions noted.
	SiteCare has implemented processes to change cryptographic keys periodically based on a defined schedule.	Inspected SiteCare, LLC's Encryption Policy to determine that it has implemented processes to change cryptographic keys periodically based on a defined schedule.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has implemented processes to change credentials (secrets, access keys, API keys, etc.) periodically based on a defined schedule.	Inspected SiteCare, LLC's Plugin configuration to determine that it has implemented processes to change credentials (secrets, access keys, API keys, etc.) periodically based on a defined schedule.	No exceptions noted.
	SiteCare has a documented policy that establishes requirements for the use of cryptographic controls.	Inspected SiteCare, LLC's Encryption Policy to determine that SiteCare has a documented policy that establishes requirements for the use of cryptographic controls.	No exceptions noted.
	Data in transit is encrypted using strong cryptographic algorithms.	Inspected SiteCare, LLC's web certificate to determine that data in transit is encrypted using strong cryptographic algorithms.	No exceptions noted.
CC 6.2 - Before issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	SiteCare has developed and documented a policy that outlines requirements for access control.	Inspected SiteCare, LLC's Employees Acceptance of the Policy to determine that SiteCare has developed and documented a policy that outlines requirements for access control.	No exceptions noted.
	Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected SiteCare, LLC's system access review to determine that SiteCare, LLC management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	No exceptions noted.
	System and physical access are revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	Obtained a sample of the list of terminated employees by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's access is revoked to determine that system and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	No exceptions noted.
	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's data access to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	SiteCare has developed and documented a policy that outlines requirements for access control.	Inspected SiteCare, LLC's Employees' Acceptance of the Policy to determine that SiteCare has developed and documented a policy that outlines requirements for access control.	No exceptions noted.
	Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected SiteCare, LLC's system access review to determine that SiteCare, LLC management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.	No exceptions noted.
	System and physical access are revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	Obtained a sample of the list of terminated employees by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's access is revoked to determine that system and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third-party vendors, and other personnel).	No exceptions noted.
	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Obtained a sample of the list of new hires by SiteCare, LLC, during the audit period. Inspected SiteCare, LLC's data access to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
	SiteCare assigns permissions to accounts based on the principle of least privilege and limits the use of wildcard permissions or broad-access patterns.	Inspected SiteCare, LLC's user role assignments to determine that SiteCare, LLC assigns permissions to accounts based on the principle of least privilege and limits the use of wildcard permissions or broad-access patterns.	No exceptions noted.
CC 6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The entity does not operate any physical hardware, such as servers and network devices, but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is implemented and maintained by sub-service organizations.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected SiteCare, LLC's Certification of Secure Hard Disk Drive Wiping to determine that SiteCare has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted.
	When SiteCare disposes of hard copy materials, it does so through secure means such as cross-cut shredding, incinerating, or pulping, so that sensitive data cannot be reconstructed.	Inspected SiteCare, LLC's Hard Copy Disposal to determine that SiteCare disposes of hard copy materials. It does so through secure means such as cross-cut shredding, incinerating, or pulping so that sensitive data cannot be reconstructed.	No exceptions noted.
	SiteCare has documented policies and procedures for the erasure or destruction of information that has been identified for disposal.	Inspected SiteCare, LLC's Erasure and Destruction of Information Process to determine that SiteCare, LLC has documented policies and procedures for the erasure or destruction of information that has been identified for disposal.	No exceptions noted.
	A mobile device management (MDM) is installed in company-issued devices and bring-your-own devices used for company purposes to enforce security for assets off-premise (e.g., location tracking, remote locking and wiping, threat detection, restrictions on software installation, etc.).	Inspected SiteCare, LLC's Mobile Device Management Software to determine that SiteCare, LLC mobile device management (MDM) is installed in company-issued devices and bring-your-own devices used for company purposes to enforce security for assets off-premise (e.g., location tracking, remote locking and wiping, threat detection, restrictions on software installation, etc.).	No exceptions noted.
CC 6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Company-managed devices are configured to enforce a screensaver lock after a defined period of inactivity in accordance with company policies and compliance requirements.	Inspected SiteCare, LLC's screen lock configuration to determine that SiteCare, LLC ensures that company-managed devices are configured to enforce a screensaver lock after a defined period of inactivity in accordance with company policies and compliance requirements.	No exceptions noted.
	Data in transit is encrypted using strong cryptographic algorithms.	Inspected SiteCare, LLC's web certificate to determine that data in transit is encrypted using strong cryptographic algorithms.	No exceptions noted.
	SiteCare has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected SiteCare, LLC's Password Configurations to determine that SiteCare, LLC has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	No exceptions noted.
	Authentication to systems requires the use of multi-factor authentication.	Inspected SiteCare, LLC's Multi-Factor Authentication and verified the use of automated continuous control monitoring to determine that authentication to systems requires the use of multi-factor authentication.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected SiteCare, LLC's intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent to determine that it is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.
	Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.	Inspected SiteCare, LLC's Digital Ocean Firewall Configuration and verified the use of automated continuous control monitoring to determine that network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.	No exceptions noted.
	Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.).	Inspected SiteCare, LLC's remote access to production systems to determine that it is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.).	No exceptions noted.
	A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected SiteCare, LLC's threat detection system to determine that it is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
	A web application firewall is in place to protect public-facing web applications from outside threats.	Inspected SiteCare, LLC's web application firewall and verified the use of automated continuous control monitoring to determine that it is in place to protect public-facing web applications from outside threats.	No exceptions noted.
	Data at rest is encrypted using strong cryptographic algorithms.	Inspected SiteCare, LLC's infrastructure data encryption to determine that data at rest is encrypted using strong cryptographic algorithms.	No exceptions noted.
	All remote access to the entityâ€™s network (including that of users, administrators, and third parties or vendors) requires multi-factor authentication.	Inspected SiteCare, LLC's Multi-Factor Authentication to determine that all remote access to the entityâ€™s network (including that of users, administrators, and third parties or vendors) requires multi-factor authentication.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Data in transit is encrypted using strong cryptographic algorithms.	Inspected SiteCare, LLC's web certificate to determine that data in transit is encrypted using strong cryptographic algorithms.	No exceptions noted.
	Hard-disk encryption is enabled on all company-managed devices.	Inspected SiteCare, LLC's hard disk encryption to determine that it is enabled on all company-managed devices.	No exceptions noted.
	SiteCare has implemented data leakage prevention mechanisms in systems that process, store, or transmit sensitive information. These mechanisms are configured to prevent data leakage and generate audit logs and alerts.	Inspected SiteCare, LLC's Data Protection Policy and DLP configuration to determine that SiteCare has implemented data leakage prevention mechanisms in systems that process, store, or transmit sensitive information. These mechanisms are configured to prevent data leakage and generate audit logs and alerts.	No exceptions noted.
	Automated operating system (OS) updates are enabled on company-managed devices to install security patches.	Inspected SiteCare, LLC's automated operating system (OS) updates to determine that they are enabled on company-managed devices to install security patches.	No exceptions noted.
	SiteCare has documented a policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data.	Obtained a sample of new hires by SiteCare, LLC during the audit period. Inspected SiteCare, LLC's Data Protection Policy to determine that has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data.	No exceptions noted.
	All media with sensitive data is encrypted and/or physically secured to prevent unauthorized persons from gaining access to the data.	Inspected SiteCare, LLC's Data Protection Policy to determine that all media with sensitive data is encrypted and/or physically secured to prevent unauthorized persons from gaining access to the data.	No exceptions noted.
CC 6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	SiteCare has implemented automated mechanisms (e.g., unattended-upgrades, automated patching tools, etc.) to install security fixes to systems.	Inspected SiteCare, LLC's automated security updates to determine that they have implemented automated mechanisms (e.g., unattended-upgrades, automated patching tools, etc.) to install security fixes to systems.	No exceptions noted.
	A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected SiteCare, LLC's threat detection system to determine that it is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Antimalware software is installed on all company-managed devices.	Inspected SiteCare, LLC's antivirus installed on employee workstation and verified the use of automated continuous control monitoring to determine that SiteCare requires antimalware software to be installed on all company-managed devices.	No exceptions noted.
	The deployed anti-malware solution is configured to detect all known types of malware and to remove, block, or contain all known types of malware, and is kept current via automatic updates.	Inspected SiteCare, LLC's anti-malware to determine that the deployed anti-malware solution is configured to detect all known types of malware and to remove, block, or contain all known types of malware, and is kept current via automatic updates.	No exceptions noted.
	The implemented anti-malware solutions are configured to perform periodic scans and active or real-time scans or perform continuous behavioral analyses of systems or processes.	Inspected SiteCare, LLC's anti-malware to determine that implemented anti-malware solutions are configured to perform periodic scans and active or real-time scans or perform continuous behavioral analyses of systems or processes.	No exceptions noted.
	Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	Inspected SiteCare, LLC's Change Management Policy to determine that changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	No exceptions noted.
	SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected SiteCare, LLC's security panel to determine that SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	No exceptions noted.
	The implemented anti-malware solutions are configured to perform automatic scans or continuous behavioral analysis of systems or processes when removable electronic media is inserted, connected, or logically mounted within the environment.	Inspected SiteCare, LLC's Avast external storage scan configuration to determine that SiteCare-implemented anti-malware solutions are configured to perform automatic scans or continuous behavioral analysis of systems or processes when removable electronic media is inserted, connected, or logically mounted within the environment.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Access to manage utility programs (including anti-virus consoles and diagnostic, patching, backup, or network tools, or any other utility that can be capable of overriding system and application controls) is restricted to authorized system administrators. Standard users cannot disable privileged utilities or modify their configurations.	Inspected SiteCare, LLC's Administrative Users to determine that SiteCare, LLC access to manage utility programs (including anti-virus consoles and diagnostic, patching, backup, or network tools, or any other utility can be capable of overriding system and application controls) is restricted to authorized system administrators. Standard users cannot disable privileged utilities or modify their configurations.	No exceptions noted.
	A mobile device management (MDM) is installed in company-issued devices and bring-your-own devices used for company purposes to enforce security for assets off-premise (e.g., location tracking, remote locking and wiping, threat detection, restrictions on software installation, etc.).	Inspected SiteCare, LLC's Mobile Device Management Software to determine that SiteCare, LLC mobile device management (MDM) is installed in company-issued devices and bring-your-own devices used for company purposes to enforce security for assets off-premise (e.g., location tracking, remote locking and wiping, threat detection, restrictions on software installation, etc.).	No exceptions noted.
CC 7.0 - System Operations			
CC 7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	SiteCare conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel, and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected SiteCare, LLC's vulnerability scan to determine that SiteCare, LLC conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel, and vulnerabilities are tracked to resolution in accordance with company policies.	No exceptions noted.
	A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected SiteCare, LLC's threat detection system to determine that it is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
	An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected SiteCare, LLC's intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent to determine that it is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Production systems and resources are monitored, and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	Inspected SiteCare, LLC's system access monitoring to determine that production systems and resources are monitored, and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	No exceptions noted.
	SiteCare has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.).	Inspected SiteCare, LLC's hardening standards that are in place to determine that SiteCare has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.).	No exceptions noted.
	Automated operating system (OS) updates are enabled on company-managed devices to install security patches.	Inspected SiteCare, LLC's automated operating system (OS) updates to determine that they are enabled on company-managed devices to install security patches.	No exceptions noted.
	Storage buckets that contain sensitive data have versioning enabled to preserve, retrieve, and restore versions of objects.	Inspected SiteCare, LLC's storage buckets to determine that they contain sensitive data and have versioning enabled to preserve, retrieve, and restore versions of objects.	No exceptions noted.
	SiteCare has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected SiteCare, LLC's Vulnerability Management Policy to determine that SiteCare has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
	SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected SiteCare, LLC's security panel to determine that SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare uses static application security testing (SAST) or an equivalent tool as part of the CI/CD pipeline to detect vulnerabilities in the codebase. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of the vulnerability.	Inspected SiteCare, LLC's static application security testing (SAST) to determine that SiteCare, LLC uses testing or equivalent tools as part of the CI/CD pipeline to detect vulnerabilities in the codebase. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of the vulnerability.	No exceptions noted.
	SiteCare checks software components and libraries for policy and license compliance, security risks, and supported versions (e.g., using software composition analysis (SCA) tools in the development pipeline, etc.). If vulnerabilities in these software components or libraries are identified, fixes are implemented in accordance with the company's vulnerability management policies.	Inspected SiteCare, LLC's software composition analysis to determine that SiteCare, LLC checks software components and libraries for policy and license compliance, security risks, and supported versions (e.g., using software composition analysis (SCA) tools in the development pipeline, etc.). If vulnerabilities in these software components or libraries are identified, fixes are implemented in accordance with the company's vulnerability management policies.	No exceptions noted.
	SiteCare maintains secure and supported configuration standards for application and platform runtimes.	Inspected SiteCare, LLC's OS Security patches to determine that SiteCare, LLC maintains secure and supported configuration standards for application and platform runtimes.	No exceptions noted.
	Antimalware software is installed on all company-managed devices.	Inspected SiteCare, LLC's antivirus installed on employee workstation and verified the use of automated continuous control monitoring to determine that SiteCare requires antimalware software to be installed on all company-managed devices.	No exceptions noted.
CC 7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected SiteCare, LLC's threat detection system to determine that it is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
	SiteCare uses a system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel.	Inspected SiteCare, LLC's security monitoring to determine that SiteCare, LLC uses a system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Production systems and resources are monitored, and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	Inspected SiteCare, LLC's system access monitoring to determine that production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalate per policy if necessary.	No exceptions noted.
	An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected SiteCare, LLC's intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent to determine that it is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.
	A web application firewall is in place to protect public-facing web applications from outside threats.	Inspected SiteCare, LLC's web application firewall and verified the use of automated continuous control monitoring to determine that it is in place to protect public-facing web applications from outside threats.	No exceptions noted.
	Audit logs are enabled and active for all system components and sensitive data in accordance with company policies.	Inspected SiteCare, LLC's logging and monitoring policy to determine that SiteCare audit logs are enabled and active for all system components and sensitive data in accordance with company policies.	No exceptions noted.
	Automated audit trails or logs are implemented for all system components to capture all actions taken by any individual with administrative access, including any interactive use of applications or system accounts.	Inspected SiteCare, LLC's audit trail to determine that automated audit trails or logs are implemented for all system components to capture all actions taken by any individual with administrative access, including any interactive use of applications or system accounts.	No exceptions noted.
	Automated audit trails or logs are implemented for all system components to capture all invalid access attempts.	Inspected SiteCare, LLC's audit trails to determine that automated audit trails or logs are implemented for all system components to capture all invalid access attempts.	No exceptions noted.
	Automated audit trails or logs are implemented to capture all changes to identification and authentication credentials (e.g., creation of new accounts, elevation of privileges, changes, additions, or deletions to accounts with administrative access, etc.).	Inspected SiteCare, LLC's audit trail for identification and authentication to determine that automated audit trails or logs are implemented to capture all changes to identification and authentication credentials (e.g., creation of new accounts, elevation of privileges, changes, additions, or deletions to accounts with administrative access, etc.).	No exceptions noted.
	SiteCare has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected SiteCare, LLC's Logging and Monitoring Policy to determine that it has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare has configured audit logs to trace each action to an individual user. Audit logs contain user identification, type of event, date and time, success and failure indication, origination of event, identity or name of affected data, and system component, resource, or service.	Inspected SiteCare, LLC's audit logs to determine that it has configured audit logs to trace each action to an individual user. Audit logs contain user identification, type of event, date and time, success and failure indication, origination of event, identity or name of affected data, and system component, resource, or service.	No exceptions noted.
CC 7.3 - The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	SiteCare has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	No exceptions noted.
	SiteCare has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	Inspected SiteCare, LLC's Incident Response Team to determine that SiteCare, LLC has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	No exceptions noted.
	SiteCare evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	No exceptions noted.
	SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Inspected SiteCare, LLC's Lessons Learned Documented to determine that SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	No exceptions noted.
	SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	Inspected SiteCare, LLC's Security Notice to determine that SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	SiteCare has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	No exceptions noted.
	SiteCare has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	Inspected SiteCare, LLC's Incident Response Team to determine that SiteCare, LLC has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	No exceptions noted.
	SiteCare evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	No exceptions noted.
	SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Inspected SiteCare, LLC's Lessons Learned Documented to determine that SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	No exceptions noted.
	SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	Inspected SiteCare, LLC's Security Notice to determine that SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
CC 7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	SiteCare has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	No exceptions noted.
	SiteCare has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare, LLC evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.	No exceptions noted.
	SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Inspected SiteCare, LLC's Lessons Learned Documented to determine that SiteCare documents a post-mortem review for identified incidents that include root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	No exceptions noted.
	SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	Inspected SiteCare, LLC's Security Notice to determine that SiteCare provides notices of breaches and incidents to affected parties, organizational officials, and authorities in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
CC 8.0 - Change Management			
CC 8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes are tested in an environment separate from production prior to deployment in accordance with the nature of the change. Documented evidence of testing criteria and testing results is retained.	Inspected SiteCare, LLC's software development change control to determine that the changes are tested in an environment separate from production prior to deployment in accordance with the nature of the change. Documented evidence of testing criteria and testing results is retained.	No exceptions noted.
	Change releases are approved by authorized personnel prior to deployment to production.	Inspected SiteCare, LLC's change release to determine that change releases are approved by authorized personnel prior to deployment to production.	No exceptions noted.
	SiteCare has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating software development changes.	Inspected SiteCare, LLC's Software Development Lifecycle Policy to determine that they have developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating software development changes.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Inspected SiteCare, LLC's version control tool and verified the use of automated continuous control monitoring to determine that it manages source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	No exceptions noted.
	Access to make changes in production environments is restricted to authorized personnel in accordance with the segregation of duties principles and the company's documented policies and procedures.	Inspected SiteCare, LLC's change deployers and verified the use of automated continuous control monitoring to determine that Access to make changes in production environments is restricted to authorized personnel in accordance with the segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
	Changes are peer-reviewed and approved prior to deployment by an individual different from the developer to maintain segregation of duties. Review requirements are enforced through automated mechanisms such as branch protection settings in the production code repository.	Inspected SiteCare, LLC's change review and verified the use of automated continuous control monitoring to determine that Changes are peer-reviewed and approved prior to deployment by an individual different from the developer to maintain segregation of duties. Review requirements are enforced through automated mechanisms such as branch protection settings in the production code repository.	No exceptions noted.
	Emergency changes or hotfixes implemented outside of the standard change management process are reviewed and approved by an authorized individual after implementation.	Inspected SiteCare, LLC's Change Management Policy to determine that emergency changes or hotfixes implemented outside of the standard change management process are reviewed and approved by an authorized individual after implementation.	No exceptions noted.
	Test data is used in testing and development environments to prevent sensitive information from being copied to non-production environments.	Inspected SiteCare, LLC's test data to determine that it is used in testing and development environments to prevent sensitive information from being copied to non-production environments.	No exceptions noted.
	SiteCare has implemented automated mechanisms (e.g., unattended-upgrades, automated patching tools, etc.) to install security fixes to systems.	Inspected SiteCare, LLC's automated security updates to determine that they have implemented automated mechanisms (e.g., unattended-upgrades, automated patching tools, etc.) to install security fixes to systems.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	Inspected SiteCare, LLC's Change Management Policy to determine that changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including security impact testing).	No exceptions noted.
	SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected SiteCare, LLC's security panel to determine that SiteCare has enabled file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	No exceptions noted.
	SiteCare has a documented policy that describes the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	Inspected SiteCare, LLC's Change Management Policy to determine that SiteCare has a documented policy that describes the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	No exceptions noted.
	SiteCare has implemented a software update management process where critical patches and application updates are installed for all authorized software within priority SLAs established in company policies.	Inspected SiteCare, LLC's automated operating system upgrades to determine that SiteCare, LLC has implemented a software update management process where critical patches and application updates are installed for all authorized software within priority SLAs established in company policies.	No exceptions noted.
	SiteCare uses static application security testing (SAST) or an equivalent tool as part of the CI/CD pipeline to detect vulnerabilities in the codebase. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of the vulnerability.	Inspected SiteCare, LLC's static application security testing (SAST) to determine that SiteCare, LLC uses testing or equivalent tools as part of the CI/CD pipeline to detect vulnerabilities in the codebase. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of the vulnerability.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC 9.0 - Risk Mitigation			
CC 9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	SiteCare has a documented disaster recovery plan that outlines roles, responsibilities, and detailed procedures for the recovery of systems in the event of a disaster scenario.	Inspected SiteCare, LLC's Disaster Recovery Plan to determine that it has a documented disaster recovery plan that outlines roles, responsibilities, and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
	SiteCare has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Inspected SiteCare, LLC's Incident Response Plan to determine that SiteCare has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	No exceptions noted.
	SiteCare maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	Inspected SiteCare, LLC's Cybersecurity Insurance to determine that SiteCare maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	No exceptions noted.
	Business-critical cloud resources are deployed in accordance with high-availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high availability, etc.).	Inspected SiteCare, LLC's Screenshots from AWS RDS showing that high availability is enabled and verified the use of automated continuous control monitoring to determine that SiteCare Business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.).	No exceptions noted.
	SiteCare has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected SiteCare, LLC's Business Continuity Plan to determine that SiteCare has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	No exceptions noted.
CC 9.2 - The entity assesses and manages risks associated with vendors and business partners.	SiteCare maintains a vendor/third-party register that includes a description of each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing, or managing information assets are reviewed to validate they address all relevant requirements prior to execution.	Inspected SiteCare, LLC's vendor agreement to determine that SiteCare, LLC maintains a vendor/third party register that includes a description for each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing, or managing information assets are reviewed to validate that they address all relevant requirements prior to execution.	No exceptions noted.

Trust Services Criteria	Description of SiteCare, LLC's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	SiteCare obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.), and SiteCare's requirements. Results of the review and action items, if any, are documented.	Inspected SiteCare, LLC's Directory of key vendors and verified the use of automated continuous control monitoring to determine that SiteCare, LLC obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and SiteCare's requirements. Results of the review and action items, if any, are documented.	No exceptions noted.
	SiteCare shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information.	Inspected SiteCare, LLC's vendor and data processing agreement to determine that it shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information.	No exceptions noted.
	SiteCare has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	Inspected SiteCare, LLC's Vendor Management Policy to determine that it has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	No exceptions noted.
	SiteCare has data processing agreements (DPAs) in place with sub-processors that include the minimum technical and organizational measures that the third parties need to implement to meet the objectives of SiteCare's privacy program.	Inspected SiteCare, LLC's Data Processing Agreements to determine that it has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	No exceptions noted.
	SiteCare performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures, or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities including action items are documented.	Inspected SiteCare, LLC's vendor due diligence discovery to determine that SiteCare, LLC performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures, or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities including action items are documented.	No exceptions noted.