JOHANSON GROUP

System and Organization Controls (SOC) 2 Type I Report

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security Category

As of December 09, 2024

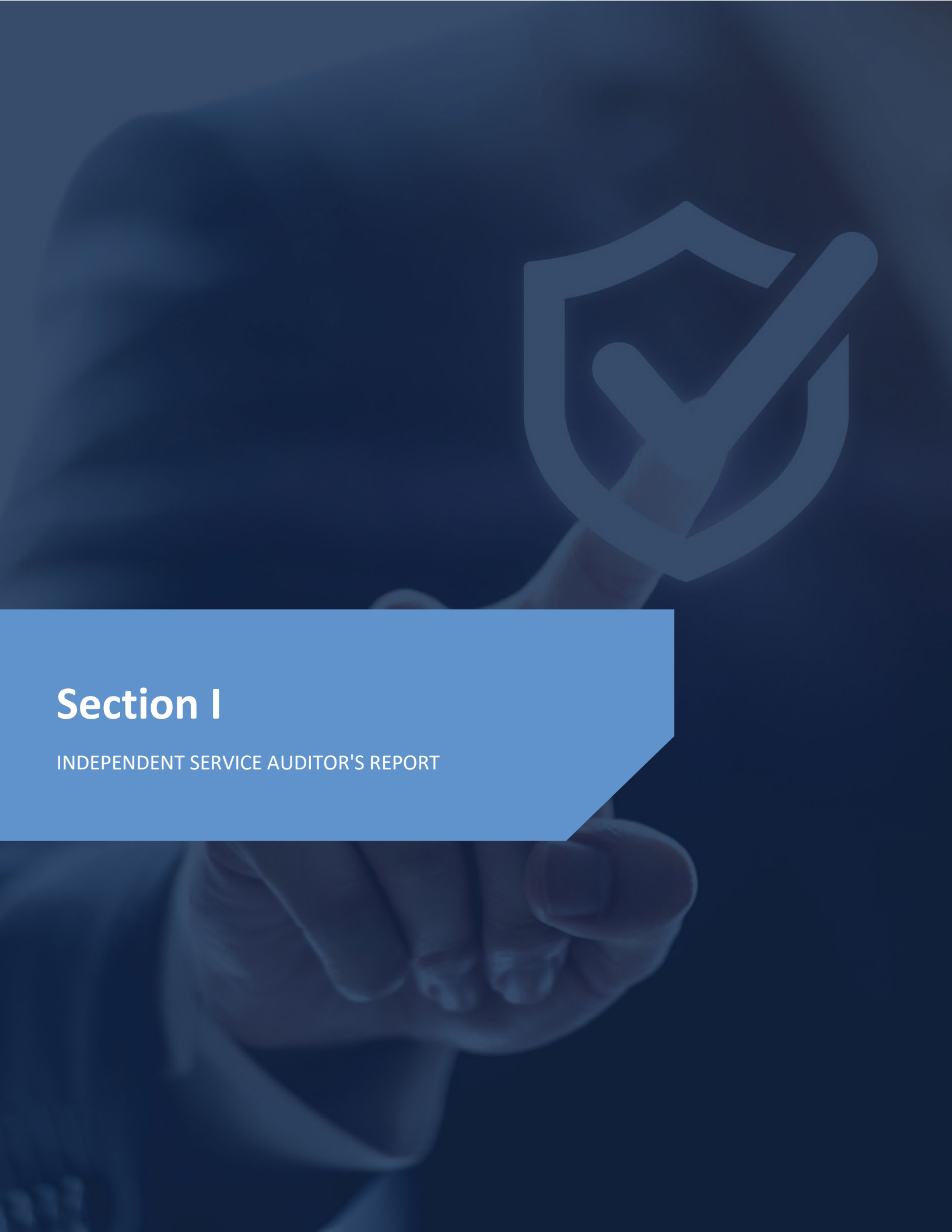
Together with Independent Service Auditor's Report

Report on Management's Description of

sitecare®

TABLE OF CONTENTS

I.	Independent Service Auditor's Report	3
II.	Assertion of SiteCare, LLC Management	7
III.	Description of SiteCare	9
IV.	Description of Design of Controls and Results Thereof	19



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" as of December 09, 2024 (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 of controls stated in the description as of December 09, 2024, to provide reasonable assurance that SiteCare, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 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 controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of SiteCare, LLC 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 the accompanying assertion titled "Assertion of SiteCare, LLC's Management" (assertion) about the description and the suitability of the design of controls stated therein. SiteCare, LLC is also 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 control design 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 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 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.
- 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.
- 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 report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents SiteCare, LLC's SiteCare (system) that was designed and implemented as of December 09, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of December 09, 2024, 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 as of that date.

Restricted Use

This report is intended solely for the information and use of SiteCare, LLC, user entities of SiteCare, LLC's SiteCare (system) as of December 09, 2024, business partners of SiteCare, LLC subject to risks arising from interactions with the SiteCare (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:

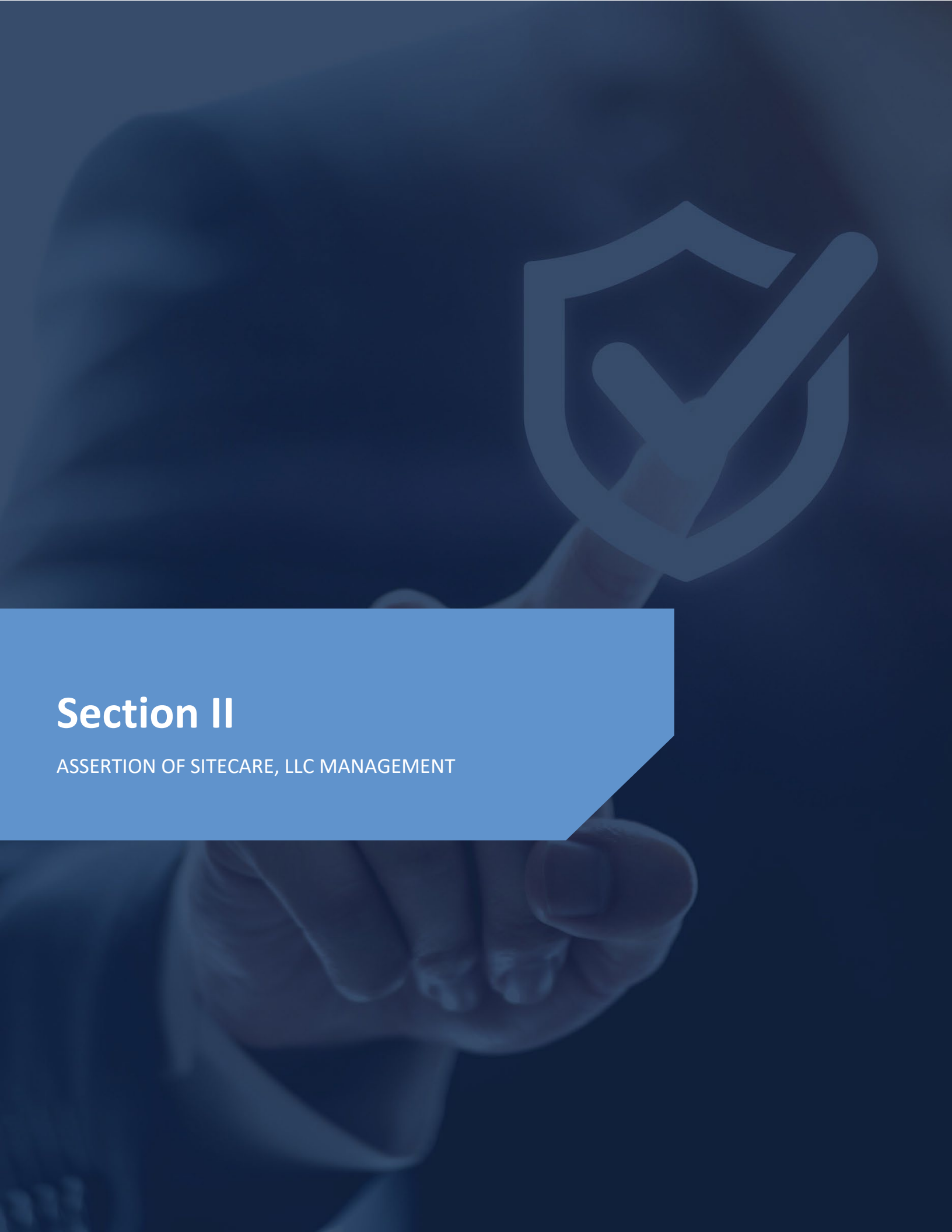
- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user 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 Springs, Colorado
January 14, 2025



Section II

ASSERTION OF SITECARE, LLC MANAGEMENT

We have prepared the accompanying description of SiteCare, LLC's SiteCare (system) titled "Description of SiteCare as of December 09, 2024," (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 the 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*.

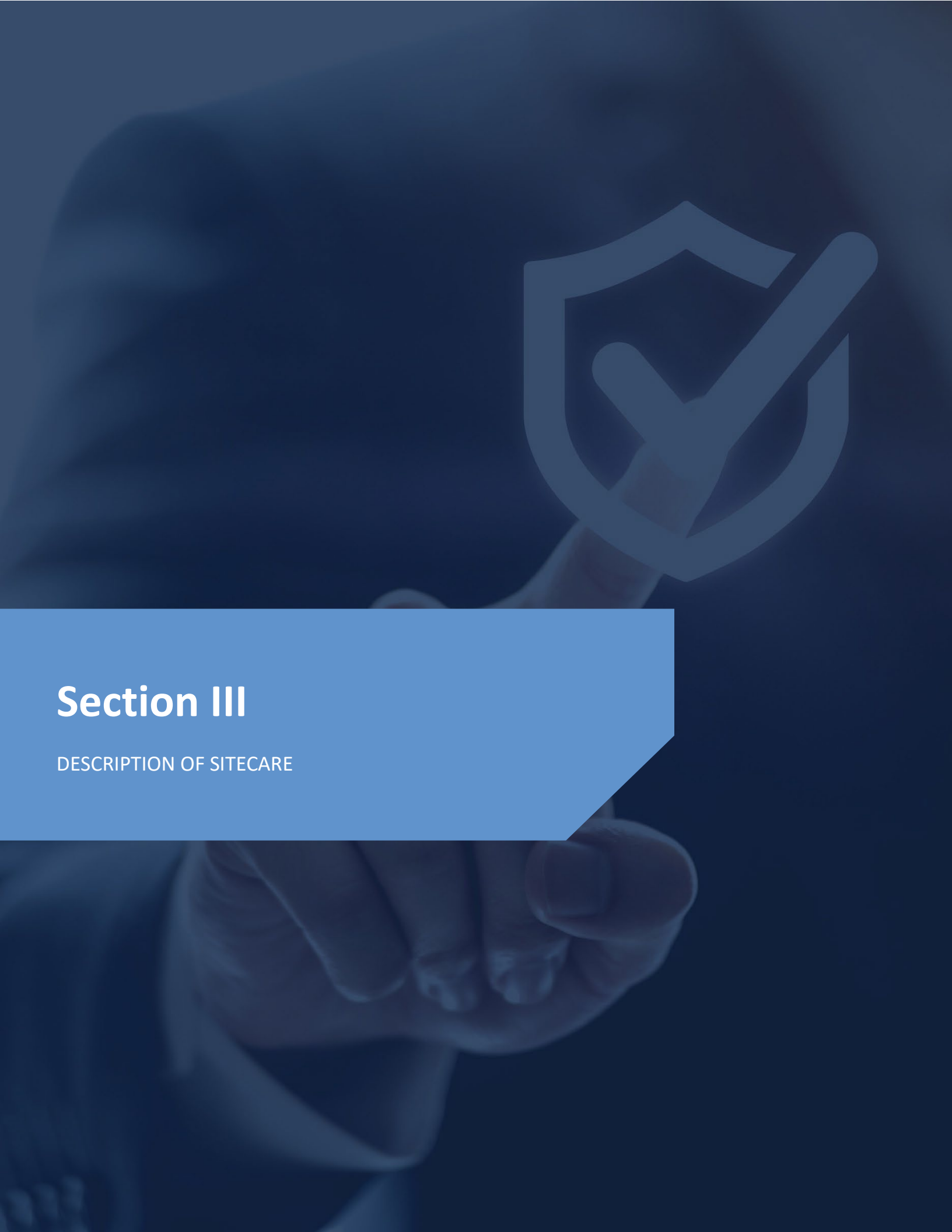
SiteCare, LLC uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SiteCare, LLC, to achieve SiteCare, 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 as of December 09, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of December 09, 2024, 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 as of that date.

SiteCare, LLC Management
January 14, 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, 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.

Subservice Organizations Providing Infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Digital Ocean	Digital Ocean Droplets	Cloud-based infrastructure for flexible and scalable server environments.

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	**Operating System**	**Purpose**
MySQL	Linux	A relational database management system is used to store and retrieve 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	The 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	Content management system (CMS) used to build, manage, and optimize client websites.

People

SiteCare's team of 12 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 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 including Digital Ocean. 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 privilege 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:

- **Administrator**: Can modify policies, provision, or de-provision users.
- **User**: Has full read/write access to the SaaS or cloud service, excluding administrative functions.
- **No Access**: No permissions granted.

Roles and permissions are reviewed annually by management to ensure adherence to least-privilege 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. 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 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 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 (SECURITY)

Common Criteria (to the Security Categories)
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 or 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 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 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 them 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

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

INCIDENTS

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

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria are 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:

- **Digital Ocean**: Deliver managed WordPress hosting platforms, including server management, storage, and scalable infrastructure to support client websites.

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 to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization - Digital Ocean		
Category	**Criteria**	**Control**
Common Criteria / 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.
		Collocated data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.

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:

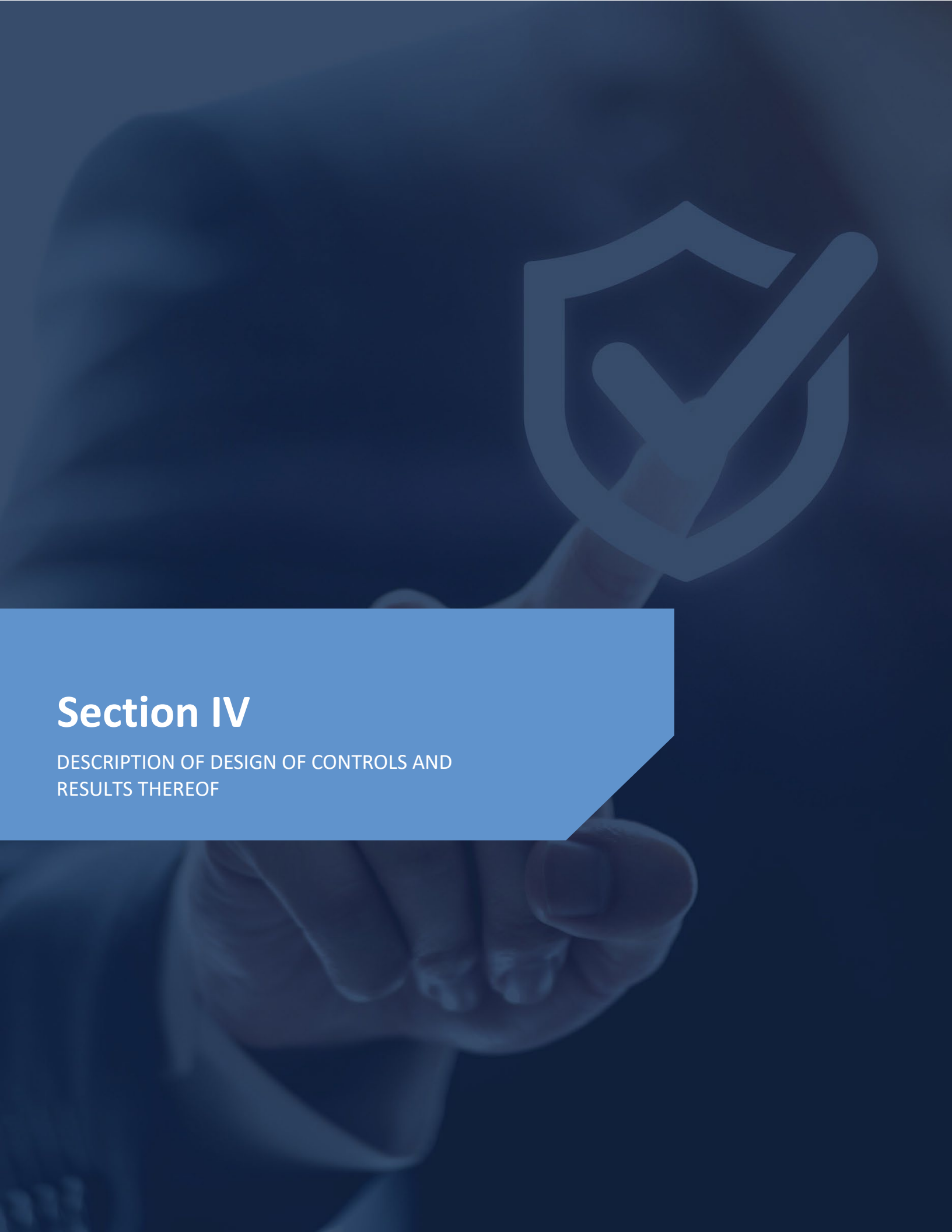
- **SiteCare's Role**: Configuring and managing client environments, monitoring performance, and addressing incidents promptly.
- **Subservice Organizations' Role**: Maintaining the physical and virtual infrastructure that supports SiteCare's operations.

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.
4. Promptly notify SiteCare of any security incidents.



Section IV

DESCRIPTION OF DESIGN 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 assessed if SiteCare, LLC's controls were suitably designed to meet 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)*, as of December 09, 2024.

Assessment of control design included inquiry of appropriate management, supervisory, and staff personnel and the inspection of SiteCare, LLC's policy and procedure documentation. The results of those assessments were considered in the planning, the nature, timing, and extent of Johanson LLP's review of the controls designed to address the relevant trust services criteria. Being a Type I SOC 2 report, there were no tests performed to determine the operational effectiveness of each designed control.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
CONTROL ENVIRONMENT			
CC 1.1	The entity demonstrates a commitment to integrity and ethical values.	The company maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
CC 1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company engages with a third party to conduct a Risk Assessment at least annually.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Control determined to be suitably designed.
CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
CC 1.4	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.	Control determined to be suitably designed.
		The company maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
CC 1.5	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.	Control determined to be suitably designed.
		The company maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.	Control determined to be suitably designed.
COMMUNICATION AND INFORMATION			
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Control determined to be suitably designed.
		The company has an established policy and procedures that govern the use of cryptographic controls.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.).	Control determined to be suitably designed.
		A documented architectural diagram is in place to document system boundaries and support the functioning of internal control. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment.	Control determined to be suitably designed.
		The company management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Control determined to be suitably designed.
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Control determined to be suitably designed.
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Control determined to be suitably designed.
		The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The security team communicates important information security events to company management promptly.	Control determined to be suitably designed.
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company maintains a publicly available privacy policy/notice.	Control determined to be suitably designed.
		Master service agreements outlining specific requirements are executed with enterprise customers or when the standard terms of service may not apply.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.	Control determined to be suitably designed.
		The company tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
RISK ASSESSMENT			
CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
CC 3.2	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.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Control determined to be suitably designed.
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Control determined to be suitably designed.
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company 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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
MONITORING ACTIVITIES			
CC 4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has developed and documented a policy that outlines requirements for access control.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
CC 4.2	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.	The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company 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.	Control determined to be suitably designed.
		The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Control determined to be suitably designed.
		The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Control determined to be suitably designed.
CONTROL ACTIVITIES			
CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Control determined to be suitably designed.
CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Control determined to be suitably designed.
		The company has an established policy and procedures that govern the use of cryptographic controls.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.	Control determined to be suitably designed.
		The company's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Control determined to be suitably designed.
CC 5.3	The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	Control determined to be suitably designed.
		The company has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Control determined to be suitably designed.
		The company maintains a documented code of conduct. Eligible personnel are required to acknowledge SiteCare's code of conduct during onboarding and annually thereafter.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
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.	Control determined to be suitably designed.
		Hard-disk encryption is enabled on all company-managed devices.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company has an established key management process in place to support the organization's use of cryptographic techniques.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		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.).	Control determined to be suitably designed.
		Authentication to systems requires the use of multi-factor authentication.	Control determined to be suitably designed.
		Data at rest is encrypted using strong cryptographic algorithms.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.).	Control determined to be suitably designed.
		Unique user IDs are used for authentication to systems.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company 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.).	Control determined to be suitably designed.
		Administrative or privileged access to systems and resources is restricted to authorized personnel.	Control determined to be suitably designed.
		Username and password (password standard implemented) or SSO required to authenticate into the application, MFA optional for external users, and MFA required for employee users.	Control determined to be suitably designed.
		Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.)	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
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.	The company has developed and documented a policy that outlines requirements for access control.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		A termination checklist is used to ensure that system access, including physical access, for terminated employees, has been removed within one specified time.	Control determined to be suitably designed.
		System and physical access are revoked within one business day of the effective termination date for terminated users (including employees, third parties vendors, and other personnel).	Control determined to be suitably designed.
		Unique user IDs are used for authentication to systems.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company maintains a publicly available term of service for use of the system. All users must agree to the terms of service prior to using the system.	Control determined to be suitably designed.
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.	The company has developed and documented a policy that outlines requirements for access control.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		A termination checklist is used to ensure that system access, including physical access, for terminated employees, has been removed within one specified time.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		System and physical access are revoked within one business day of the effective termination date for terminated users (including employees, third parties vendors, and other personnel).	Control determined to be suitably designed.
		Unique user IDs are used for authentication to systems.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		The company maintains a publicly available term of service for use of the system. All users must agree to the terms of service prior to using the system.	Control determined to be suitably designed.
		Administrative or privileged access to systems and resources is restricted to authorized personnel.	Control determined to be suitably designed.
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.	Control determined to be suitably designed.
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 disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Control determined to be suitably designed.
		A termination checklist is used to ensure that system access, including physical access, for terminated employees, has been removed within one specified time.	Control determined to be suitably designed.
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.	Control determined to be suitably designed.
		Data in transit is encrypted using strong cryptographic algorithms.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		Authentication to systems requires the use of multi-factor authentication.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.	Control determined to be suitably designed.
		Cloud resources are configured to deny public access.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		Username and password (password standard implemented) or SSO required to authenticate into the application, MFA optional for external users, and MFA required for employee users.	Control determined to be suitably designed.
		Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.)	Control determined to be suitably designed.
		A web application firewall is in place to protect public-facing web applications from outside threats.	Control determined to be suitably designed.
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.	Control determined to be suitably designed.
		Hard-disk encryption is enabled on all company-managed devices.	Control determined to be suitably designed.
		The company encrypts removable media devices, such as USB drives, digital video disks, compact disks, external or removable hard disks, etc., that contain sensitive data, to protect the confidentiality of the information during transport.	Control determined to be suitably designed.
		Data at rest is encrypted using strong cryptographic algorithms.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Control determined to be suitably designed.
		The company has implemented segregation mechanisms so that customers cannot impact or access the data or resources of other customers.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
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.	The company ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	Control determined to be suitably designed.
		The company has implemented automated mechanisms (e.g., unattended-upgrades, automated patching tools, etc.) to install security fixes to systems.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		Antimalware software is installed on all company-managed devices.	Control determined to be suitably designed.
		Automated operating system (OS) updates are enabled on company-managed devices to install security patches.	Control determined to be suitably designed.
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.	The company 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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
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.	The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		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.	Control determined to be suitably designed.
		The company is using Drata to monitor the security and compliance of its cloud infrastructure configuration.	Control determined to be suitably designed.
		The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, promptly.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
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.	The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Control determined to be suitably designed.
		The security team communicates important information security events to company management promptly.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
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.	The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Control determined to be suitably designed.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company performs a test of all components of the incident response plan and procedures at least annually through different mechanisms including simulated events. The documented plan and procedures are updated if necessary based on the results of the test.	Control determined to be suitably designed.
		The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.
		The company performs backups daily and retains them by a predefined schedule in the Backup Policy.	Control determined to be suitably designed.
		The company tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
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.	Control determined to be suitably designed.
		Change releases are approved by authorized personnel prior to deployment to production.	Control determined to be suitably designed.
		The company has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
		Pre-production environments (e.g., development, testing, etc.) are separated from production environments and the separation is enforced with access controls.	Control determined to be suitably designed.
		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.	Control determined to be suitably designed.
RISK MITIGATION			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company 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.	Control determined to be suitably designed.
		The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents.	Control determined to be suitably designed.
		The company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of SiteCare, LLC's Controls	Result
		The company 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.	Control determined to be suitably designed.
		The company maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	Control determined to be suitably designed.
		The company performs backups daily and retains them by a predefined schedule in the Backup Policy.	Control determined to be suitably designed.
		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.).	Control determined to be suitably designed.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company 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.	Control determined to be suitably designed.
		The company 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.	Control determined to be suitably designed.