SOC 2 Type I Report

As of March 18, 2026 · Public Redacted Version

ABOUT THIS DOCUMENT

This is a redacted version of CustomerNode's SOC 2 Type I report, prepared for public distribution. The independent service auditor's opinion, the management assertion, the system description, and the control matrix are preserved. The identities of specific subservice organizations and certain architectural details have been replaced with **[REDACTED]** markers.

The complete unredacted report — including subservice organization names, infrastructure topology, and vendor mappings — may be made available to current and prospective customers during security review on request to **info@customernode.com**.

AUDIT & ATTESTATION BY

Securance Pro Assurance PLLC

Firm License No. PAC-FIRM-LIC-55940

Kalispell, Montana

AICPA notice. *The SOC for Service Organizations — Service Organizations Logo may be used for twelve (12) months following the date of the report issued by a licensed CPA. After twelve months, use must cease until a new report is issued.*

SECTION 1

Management's Assertion

We have prepared the accompanying description of CustomerNode ("CustomerNode" or the company) systems as of March 18, 2026, based on the criteria for a description of a service organization's systems set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2(R) Report. The description is intended to provide report users with information about CustomerNode systems that may be useful when assessing the risks arising from interactions with CustomerNode systems, particularly information about system controls that CustomerNode has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CustomerNode utilizes [REDACTED] as its primary cloud hosting provider and [REDACTED] as a subservice organization for offsite data backup storage. The description indicates that complementary subservice organization controls at these providers, which are suitably designed and operating effectively, are necessary to achieve CustomerNode's service commitments and system requirements based on the applicable trust services criteria. The description presents CustomerNode's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CustomerNode'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 CustomerNode, to achieve CustomerNode service commitments and system requirements based on the applicable trust services criteria.

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

a) The description presents CustomerNode systems that were designed as of March 18, 2026, in accordance with the description criteria.

b) The controls stated in the description were suitably designed as of March 18, 2026, to provide reasonable assurance that CustomerNode service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Michael Cantow
CEO, CustomerNode

SECTION 2

Independent Service Auditor's Report

To: CustomerNode

Scope

We have examined CustomerNode ("CustomerNode") accompanying description of its system as of March 18, 2026, 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(R) Report, and the suitability of the design of controls stated in the description as of March 18, 2026, to provide reasonable assurance that CustomerNode service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CustomerNode uses [REDACTED] cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CustomerNode, to achieve its service commitments and system requirements based on the applicable trust services criteria. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

Service Organization's Responsibilities

CustomerNode 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 CustomerNode service commitments and system requirements were achieved.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

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.

Opinion

In our opinion, in all material respects:

a) The description presents the CustomerNode system that was designed as of March 18, 2026 in accordance with the description criteria.

b) The controls stated in the description were suitably designed as of March 18, 2026, to provide reasonable assurance that CustomerNode'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 CustomerNode, user entities of CustomerNode system as of March 18, 2026, business partners of CustomerNode subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators.

Securance Pro Assurance PLLC
Kalispell, Montana

Firm License No.: PAC-FIRM-LIC-55940

Digitally signed 2026-04-13

SECTION 3

System Description

DC 1: Company Background

CustomerNode is a SaaS platform that turns complex, multi-stage B2B deals into executable customer-journey workflows guided from discovery to mutual success. It combines an interactive circular journey navigator, AI-driven template creation and editing, and shared collaborative spaces for buying and selling teams, with deployment options including Lightning Mode and Enterprise Mode.

The company operates as a remote workforce led by the CEO, uses [REDACTED] for sign-in, and handles customer PII, employee data, and intellectual property with data located in North America.

DC 2: Principal Service Commitments and System Requirements

CustomerNode designs its processes and procedures to meet service commitments to user entities, applicable laws and regulations, and internal financial, operational, and compliance requirements. Commitments cover security, confidentiality, and availability.

Security commitments include:

• System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.

• Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.

• Regular vulnerability scans over the system and network, and annual penetration test.

• Operational procedures for managing security incidents and breaches, including notification procedures.

• Use of encryption technologies to protect customer data both at rest and in transit.

• Data retention and data disposal.

• Uptime availability of production systems.

• Separation of duties for sensitive roles and functions.

Confidentiality commitments include:

• Use of encryption technologies to protect system data both at rest and in transit.

• Confidentiality and non-disclosure agreements with employees, contractors, and third parties.

• Confidential information may be used only for the purposes explicitly stated in agreements between CustomerNode and user entities.

Availability commitments include:

• System performance and availability monitoring mechanisms to help ensure consistent delivery of the system and its components.

• Responding to customer requests in a timely manner.

• Business continuity and disaster recovery plans.

• Operational procedures supporting the achievement of availability commitments to user entities.

DC 3: Components of the System

Infrastructure

CustomerNode maintains a system inventory that includes computers (desktops and laptops). The inventory documents device name, inventory type, description, and owner. Network topology is documented internally; specifics are [REDACTED] in this public version.

Software

CustomerNode is responsible for managing the development and operation of the CustomerNode platform, including infrastructure components such as containers, databases, and storage systems. The in-scope SaaS and IaaS components are [REDACTED] in this public version. They span identity, content delivery and edge services, edge security, and cloud object storage.

People

CustomerNode utilizes a dedicated structure to handle major product functions, including operations and support. The founder monitors the environment and manages data backups and recovery. CustomerNode is led by a principal officer organized across the following functional areas: Management (led by the CEO), Operations, Information Technology, and Product Development. Access to the production environment is restricted to the Operations functional role.

Data

Data categories include public information (press releases, public website), internal information (memos, design documents, product specifications, correspondences), customer data (operating data, customer PII, customers' customers' PII, anything subject to a confidentiality agreement), and company data (legal documents, contractual agreements, employee PII, compensation data). Customer data is managed, processed, and stored in accordance with applicable data protection regulations, with specific requirements established in customer agreements where applicable.

DC 3.5: Processes and Procedures

Physical security

CustomerNode's production servers are maintained by [REDACTED]. Physical and environmental security protections are the responsibility of [REDACTED]. CustomerNode reviews the attestation reports and performs a risk analysis of [REDACTED] on at least an annual basis.

Logical access

CustomerNode provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access. Access is split into admin roles, user roles, and no-access roles. User access and roles are reviewed annually. Provisioning includes background check, policy acknowledgement, and security training within 30 days of hire. Termination triggers deprovisioning within 1 business day.

Computer operations — backups

Customer data is backed up and monitored by DevOps for completion and exceptions. Exceptions trigger root-cause investigation and a rerun. Backup infrastructure is maintained at [REDACTED] with physical access restricted according to policy. Backups are encrypted; access is restricted to key personnel.

Computer operations — availability

CustomerNode maintains an incident response plan for reporting and responding to information security and data privacy events. Production systems are monitored for delivery against SLA requirements. Vulnerability scanning checks source code and open-source dependencies against an internal SLA for response.

Change management

CustomerNode maintains documented SDLC policies and procedures. Change control covers change request and initiation, documentation, development practices, QA testing, and approval. A ticketing system tracks change control records. Development and testing are logically separated from production. Management approves changes prior to production migration. Version control software maintains source code versions and rollback history.

Data communications

CustomerNode runs production infrastructure on [REDACTED], which simplifies network configuration by enforcing a firewall around application containers, with ingress restricted to HTTPS connections to designated web frontend endpoints. Container provisioning and replacement are automated against a desired configuration. Multiple vulnerability scanning tools are used; patch timing is risk-based and considers public exploit availability.

DC 4: Disclosures about identified security incidents

No significant security incidents affecting user entities occurred in the three months preceding the review date.

DC 7: Complementary Subservice Organization Controls

CustomerNode uses subservice organizations for cloud hosting and offsite backup storage. Specific identities are [REDACTED] in this public version. Expected complementary controls are summarized below by category.

Expected control	Subservice category	Applicable criteria
Logical access to underlying network and virtualization management software is appropriate.	Cloud hosting [REDACTED]	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to data center facility restricted to authorized personnel.	Cloud hosting [REDACTED]	CC6.4, CC6.5

Expected control	Subservice category	Applicable criteria
Environmental protection (monitoring, alarming) addresses physical security and environmental control requirements.	Cloud hosting [REDACTED]	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	Cloud hosting [REDACTED]	A1.3
Defined Data Classification Policy specifies classification levels and control requirements for confidentiality.	Cloud hosting [REDACTED]	C1.1
Defined process to sanitize and destroy hard drives and backup media before leaving company facilities.	Cloud hosting [REDACTED]	C1.2
Physical access to backup storage facility restricted to authorized personnel.	Backup storage [REDACTED]	CC6.4, CC6.5
Logical access to backup storage infrastructure and management software is appropriate.	Backup storage [REDACTED]	CC6.1, CC6.2, CC6.3, CC6.5
Backup data is encrypted at rest to protect confidentiality.	Backup storage [REDACTED]	CC6.7, C1.1
Defined process to sanitize and destroy backup media containing customer data.	Backup storage [REDACTED]	C1.2

DC 9: Significant Changes (last 3 months)

No significant changes impacting user entities occurred in the three months preceding the review date.

SECTION 4

Testing Matrix — Trust Services Criteria and Related Controls

The following table presents the applicable Trust Services Criteria and the related control activities. Generic control language is preserved verbatim from the audit; references to specific monitoring or vendor systems are [REDACTED] in this public version.

Control Environment

Trust ID	Control Description
CC1.1	Established procedures for staff to acknowledge applicable company policies periodically.
CC1.1	Established procedures for new staff to acknowledge applicable company policies during onboarding.
CC1.1	Documented policy defining behavioral standards and acceptable business conduct.
CC1.1	Documented cybersecurity responsibilities for all personnel.

Trust ID	Control Description
CC1.2	Senior Management reviews and approves all company policies annually.
CC1.2	Senior Management reviews and approves the Organizational Chart annually.
CC1.2	Senior Management reviews and approves the Risk Assessment Report annually.
CC1.2	Senior Management reviews and approves the state of the Information Security program at planned intervals.
CC1.2	Senior Management reviews and approves the Vendor Risk Assessment Report annually.

Trust ID	Control Description
CC1.3	Mechanisms to assign and manage asset ownership responsibilities.
CC1.3	Procedures to communicate with staff about their roles and responsibilities.
CC1.3	Organizational structure defines authorities, facilitates information flow, and establishes responsibilities.
CC1.3	Compliance Program Manager appointed for planning and implementing the internal control environment.
CC1.3	Information Security Officer assigned to centrally manage the cybersecurity and privacy program.

Trust ID	Control Description
CC1.4	Procedures to perform security risk screening of individuals before authorizing access.
CC1.4	Procedures to ensure security-related positions are staffed by qualified individuals.

Trust ID	Control Description
CC1.5	Procedures for staff to acknowledge applicable company policies periodically.
CC1.5	Information security and privacy training provided to staff relevant to job function.
CC1.5	Periodic evaluation of employees in client-serving, IT, Engineering, and Information Security roles.
CC1.5	Procedures for new staff to complete security and privacy literacy training during onboarding.
CC1.5	Documents, monitors, and retains individual training activities and records.

Communication and Information

Trust ID	Control Description
CC2.1	Documented policy outlining guidelines for the disposal and retention of information.
CC2.1	Current information about services displayed on the public website.
CC2.1	All policies and procedures available to staff.
CC2.1	Documented policy and procedures for physical and logical labeling of information via data classification.
CC2.1	Systems generate information reviewed and evaluated for impact on internal controls.

Trust ID	Control Description
CC2.2	Procedures for staff to acknowledge applicable company policies periodically and during onboarding.
CC2.2	Information provided to employees on how to report failures, incidents, concerns, or complaints.
CC2.2	All policies and procedures available to staff.
CC2.2	Procedures for new staff to complete security and privacy literacy training during onboarding.
CC2.2	Individual training activities and records documented, monitored, and retained.

Trust ID	Control Description
CC2.3	Current information about services displayed on the public website.
CC2.3	Information provided to customers on how to report failures, incidents, concerns, or complaints.

Risk Assessment

Trust ID	Control Description
CC3.1	Formal risk assessment exercise performed annually per documented guidelines.

Trust ID	Control Description
CC3.2	Procedures for new staff to acknowledge applicable company policies during onboarding.
CC3.2	Formal vendor risk assessment exercise performed annually.
CC3.2	Formal risk assessment exercise performed annually.
CC3.2	Each risk is assessed and scored by likelihood and impact; risks are mapped to mitigating factors.

Trust ID	Control Description
CC3.3	Potential for fraud is considered when assessing risks; tracked as an entry in the risk matrix.

Trust ID	Control Description
CC3.4	Formal vendor risk assessment exercise performed annually.
CC3.4	Formal risk assessment exercise performed annually.
CC3.4	Each risk is assessed and scored by likelihood and impact; risks are mapped to mitigating factors.

Monitoring Activities

Trust ID	Control Description
CC4.1	Mechanisms to assign and manage asset ownership responsibilities.
CC4.1	Continuous monitoring system used to track and report the health of the information security program. (System: [REDACTED])
CC4.1	Senior Management reviews and approves all company policies annually.
CC4.1	Senior Management reviews and approves the Organizational Chart annually.
CC4.1	Senior Management reviews and approves the Risk Assessment Report annually.
CC4.1	Information Security Officer assigned to centrally manage the cybersecurity and privacy program.
CC4.1	Senior Management reviews and approves the Vendor Risk Assessment Report annually.
CC4.1	Subservice organizations periodically reviewed and evaluated.
CC4.1	Inventory of systems periodically updated and reviewed.

Trust ID	Control Description
CC4.2	Information provided to employees on how to report failures, incidents, concerns, or complaints.
CC4.2	Continuous monitoring system used to track and report the health of the information security program. (System: [REDACTED])
CC4.2	Senior Management reviews and approves all company policies annually.
CC4.2	Senior Management reviews and approves the state of the Information Security program.

Control Activities

Trust ID	Control Description
CC5.1	Documented policies and procedures establish expected behavior with regard to the control environment.
CC5.1	Senior Management segregates responsibilities and duties across the organization.
CC5.1	Guidelines for acceptable and unacceptable technology usage behaviors, including consequences.

Trust ID	Control Description
CC5.2	Continuous monitoring system used to track and report the health of the information security program. (System: [REDACTED])
CC5.2	Documented policies and procedures establish expected behavior with regard to the control environment.
CC5.2	Senior Management reviews and approves all company policies annually.
CC5.2	Senior Management reviews and approves the Organizational Chart annually.
CC5.2	Senior Management reviews and approves the Risk Assessment Report annually.
CC5.2	Infosec Officer reviews and approves the list of people with access to production console annually.
CC5.2	Senior Management reviews and approves the state of the Information Security program.
CC5.2	Senior Management reviews and approves the Vendor Risk Assessment Report annually.
CC5.2	Subservice organizations periodically reviewed and evaluated.

Trust ID	Control Description
CC5.3	Procedures for staff to acknowledge applicable company policies periodically and during onboarding.
CC5.3	Documented policies and procedures establish expected behavior with regard to the control environment.
CC5.3	All policies and procedures available to staff.

Logical and Physical Access Controls

Trust ID	Control Description
CC6.1	Logical access provisioning to critical systems requires approval from authorized personnel.
CC6.1	Documented policies and procedures to manage Access Control and authorize users for system credentials.
CC6.1	Continuous monitoring system alerts the security team to update access levels of team members whose roles have changed. (System: [REDACTED])
CC6.1	Production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
CC6.1	Senior Management or Information Security Officer periodically reviews access to critical systems.
CC6.1	Senior Management or Information Security Officer periodically reviews administrative access to critical systems.
CC6.1	Documented guidelines to manage passwords and secure login mechanisms.
CC6.1	Documented policies and procedures to manage physical and environmental security.

Trust ID	Control Description
CC6.2	Logical access provisioning to critical systems requires approval from authorized personnel.
CC6.2	Documented policies and procedures to manage Access Control and authorize users for system credentials.
CC6.2	Logical access no longer required upon termination is made inaccessible in a timely manner.

Trust ID	Control Description
CC6.3	Logical access provisioning to critical systems requires approval from authorized personnel.
CC6.3	Documented policies and procedures to manage Access Control.
CC6.3	Logical access no longer required upon termination is made inaccessible in a timely manner.
CC6.3	Senior Management or Information Security Officer periodically reviews access to critical systems.
CC6.3	Access to production databases restricted to individuals who require it.
CC6.3	Senior Management or Information Security Officer periodically reviews administrative access.

Trust ID	Control Description
CC6.4	Physical access controls performed by the subservice cloud provider. ([REDACTED])

Trust ID	Control Description
CC6.5	Documented policy provides guidance on decommissioning of information assets containing classified information.

Trust ID	Control Description
CC6.6	Endpoints with access to critical servers or data are encrypted.
CC6.6	Every production host is protected by a firewall with a deny-by-default rule.

Risk Mitigation

Trust ID	Control Description
CC9.1	Formal risk assessment exercise performed annually.
CC9.1	Each risk is scored by likelihood and impact; risks are mapped to mitigating factors.
CC9.1	Documented policies and procedures describe risk identification, assessment, and mitigation.

Trust ID	Control Description
CC9.2	Formal vendor risk assessment exercise performed annually.
CC9.2	Documented policy and procedures to manage vendors/third-party suppliers.
CC9.2	Documented policies and procedures describe risk identification, assessment, and mitigation.

Additional Criteria — Availability

Trust ID	Control Description
A1.1	Methods to continuously monitor critical assets, generate capacity alerts, and protect against denial-of-service.

Trust ID	Control Description
A1.2	Documented policy on managing Data Backups, available to relevant staff.
A1.2	User and system data backed up regularly to meet RTO/RPO; backup integrity verified.
A1.2	Backup information tested periodically to verify media reliability and information integrity.
A1.2	Documented Disaster Recovery guidelines for continuing business operations during disruptions or incidents.
A1.2	Documented policies and procedures establish guidelines for continuing business operations.

Trust ID	Control Description
A1.3	Procedures to conduct regular tests of the contingency plan.
A1.3	Backup information tested periodically.
A1.3	Documented Disaster Recovery guidelines.
A1.3	Documented policies and procedures establish guidelines for continuing business operations.

Additional Criteria — Confidentiality

Trust ID	Control Description
C1.1	Documented Information Security Policy governs confidentiality, integrity, and availability.
C1.1	Physical and logical labeling of information systems per data classification policy.
C1.1	Endpoints with access to critical servers or data are encrypted.
C1.1	Procedures for staff to acknowledge applicable company policies periodically and during onboarding.
C1.1	Cryptographic mechanisms encrypt production databases storing customer data at rest.

Trust ID	Control Description
C1.2	Documented policy provides guidance on decommissioning of information assets containing classified information.
C1.2	Documented policy outlining guidelines for the disposal and retention of information.